LA DECIMA SINFONIA

GUIDA COMPLETA ALL'OPSEC

A CURA DI:

LITTLELOVE

AGGIORNAMENTO MARZO 2021

1. Introduzione
2. Sistema Operativo
3. Crittografia
4. Attacchi RAM/Estrazione Chiavi partizione Swap
5. Cold Boot Attack/Evil Maid
6. Telefono Cellulare
7. TouchID e FaceID
8. iCloud
9. Sim card
10. Provider email
11. VPN/Proxy
12. VPS
13. Sim Prestanome
14. Tabulati telefonici
15. Setup Ideale
16. Telegram e Social
17. Metadata e File
18. Carding, Truffe, Estorsioni
19. Indirizzo di Comodo
20. Cattura da parte delle fdo
21. Perquisizione
22. Cambio Identità
23. Disposizioni circa Reati informatici e Truffe
24. Database Polizia (SDI e CED Interforze)

INTRODUZIONE

Questo libro tenterà di spiegare in modo esaustivo come curare la propria opsec, in modo da garantirvi la sicurezza che nessuna forza dell'ordine vi busserà alla porta.

La guida è aggiornata al 2021 e illustrerà tutte le tecniche d'indagine che utilizzano le forze dell'ordine al giorno d'oggi.

Le forze dell'ordine sono sempre alla ricerca di nuove tecniche sempre più avanzate, quindi ricordatevi di rimanere sempre aggiornati sulle ultime novità.
Oltre alla prevenzione ci sarà una spiegazione su cosa fare in caso le forze dell'ordine riescano a trovarvi, come comportarvi e se necessario come scappare e dove scappare.

La lettura è consigliata anche a chi ha una buona opsec

"Se c'è qualcosa che fa più schifo della vita queste sono le forze dell'ordine"

SISTEMA OPERATIVO

Quale Sistema Operativo utilizzare?

I sistemi operativi Desktop più diffusi sono i seguenti:

- **Windows**
- **MacOS**
- **Linux Based (Ubuntu, ecc..)**

Per motivi di praticità parlerò di Ubuntu ma ciò che dico sarà valido per tutte le altre distribuzioni con Kernel Linux.

I sistemi operativi che dovete utilizzare sono esclusivamente i seguenti, ognuno può sceglierne uno in base alle proprie esigenze e/o comodità.

- **Windows**
- **Ubuntu**

Perché non utilizzare MacOS?

FileVault di Apple utilizza la codifica XTS-AES-128 con una chiave a 256 bit. L'algoritmo idealmente è sicuro, però la Apple possiede un Software che permette di modificare la chiave di recupero di FileVault, sia quella per la Recovery, sia quella per gli account sul dispositivo stesso.

In caso di una perizia forense i vostri dati sarebbero a disposizione dell'autorità giudiziaria.

CRITTOGRAFIA

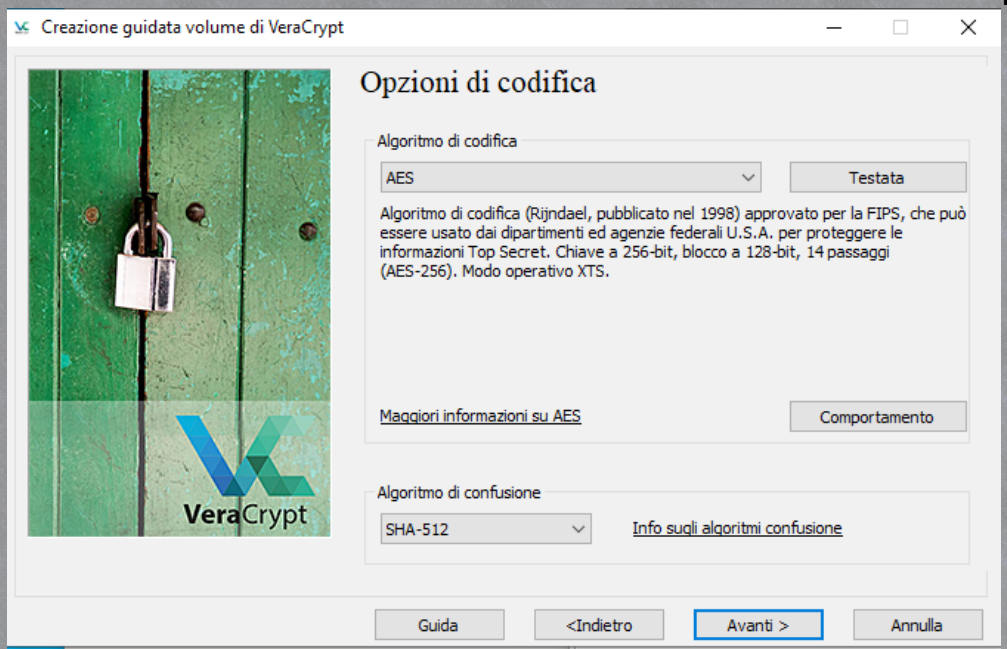
Per evitare che le forze dell'ordine estrapolino i dati dai vostri dispositivi avrete bisogno di crittografare i vostri sistemi operativi e dischi di archiviazione

- **Ubuntu**

La crittografia consigliata per Ubuntu è LUKS è possibile settare la password in fase di installazione. Consiglio una password di almeno 20+ caratteri alfanumerici

- **Windows**

Per Windows dovrete utilizzare VeraCrypt e codificare l'intero sistema operativo. Non utilizzate assolutamente Bitlocker e/o altri programmi.
VeraCrypt è attualmente il migliore.
E' sufficiente AES a 256bit, ma se siete paranoici potete utilizzare 512bit oppure algoritmi di cifratura a cascata, in modo che se in un futuro verrà violato uno resterete Bulletproof.

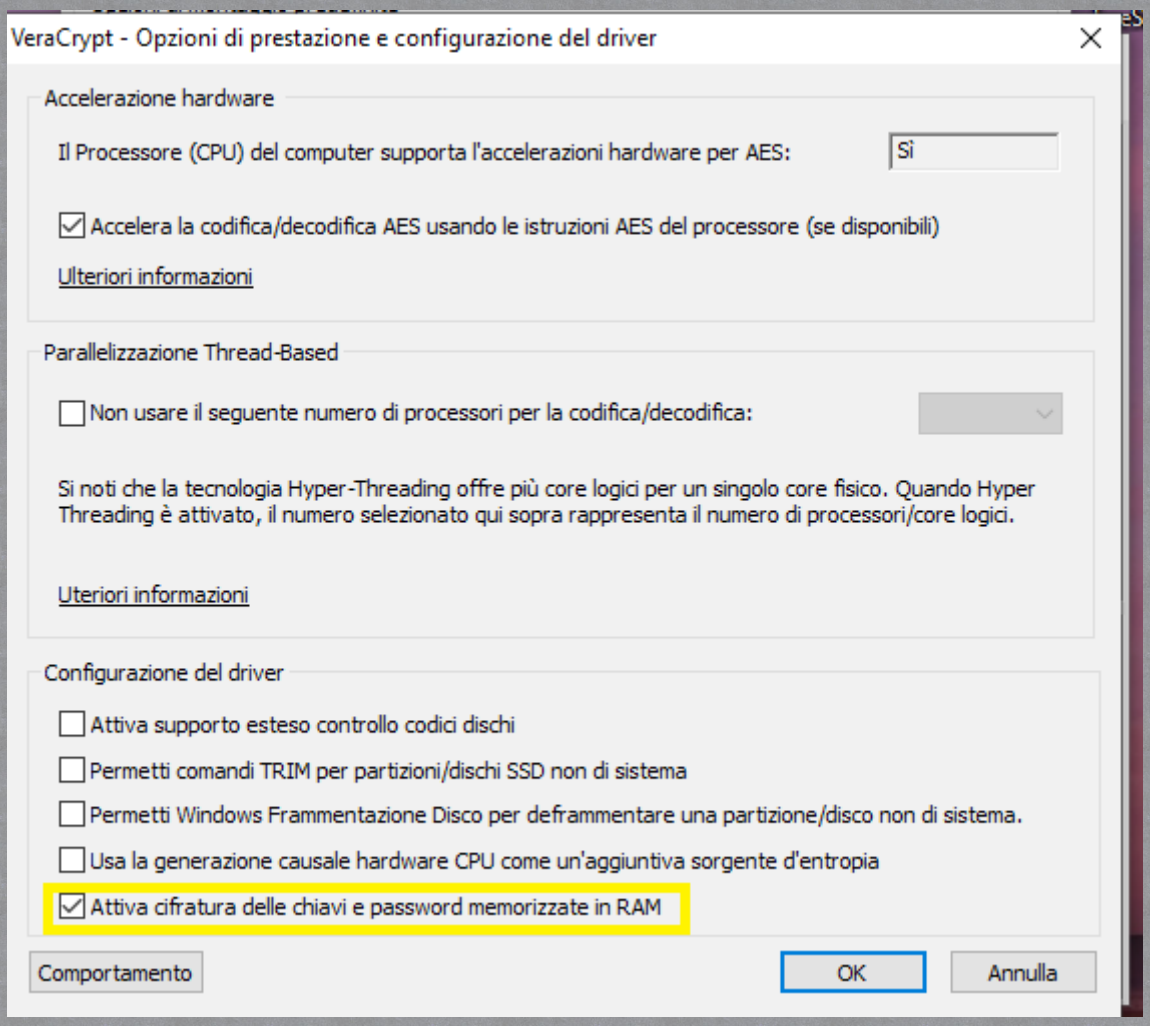


ATTACCHI RAM/ESTRAZIONE CHIAVI CRITTOGRAFICHE PARTIZIONI SWAP

Esistono diversi tipi di attacco per aggirare la crittografia dei vostri dispositivi.
I software forensi possono analizzare i file di ibernazione (hiberfil.sys su Windows) per potere recuperare le chiavi di crittografia e di conseguenza de-crittografare il vostro disco in un momento successivo, affinché questo file venga rubato dal vostro PC deve essere acceso e sbloccato.
Soluzione? Spegnere semplicemente il PC quando sospettate qualcosa, non utilizzate il PC in luoghi pubblici e/o facilmente accessibili da un affiliato alle FDO. Gli utenti più paranoici potrebbero addirittura inserire colla siliconica o tappi nelle porte USB del PC, in modo da rallentare l'eventuale operatore delle FDO e riuscire a spegnere il PC.
Le chiavi sono anche contenute nelle partizioni di swap, su Windows se utilizzate VeraCrypt sono crittografate, basterà spegnere il PC.
Su Ubuntu se durante l'installazione selezionate "Crittografa il disco", verrà crittografato tutto tranne la partizione di Swap, fate attenzione a crittografare anche quella!, sul sito di Ubuntu è presente come fare un Full Disk Encryption (quindi compresa partizione swap) o semplicemente non utilizzate la partizione di swap (Va rimossa manualmente)

COLD BOOT ATTACK/EVIL MAID

Le chiavi crittografiche sono presenti anche nelle RAM, che vengono azzerate dopo lo spegnimento del pc in circa 20 secondi. Esiste un attacco chiamato “Cold Boot Attack” che consiste nel raffreddare la RAM in modo che l’azzeramento sia rallentato tramite una sostanza refrigerante e inserire le RAM in un nuovo PC, che estrarrà tutte le informazioni dalla RAM prima che essa sia azzerata.
A volte viene Bootato un sistema operativo LIVE sul PC in questione che estrarrà anche esso tutti i dati della RAM e li salverà.
Come Prevenire questa cosa?



VeraCrypt permette la Crittografia delle chiavi in RAM, questa funzione non è attiva di Default quindi ricordatevi di attivarla!.
Ulteriore cosa da fare è incollare con colla a caldo le Ram alla scheda madre del PC in modo che la rimozione non sarà facile, sopratutto entro il tempo necessario all'azzeramento delle stesse.
Altra cosa da fare assolutamente è impostare una Password al BIOS, in modo che non possano fare BOOT tramite USB di un OS Live. Togliete completamente dalla sequenza le USB, poiché nel caso le USB siano in sequenza a loro non servirà accedere al BIOS.
Entrambi gli esempi sono sequenze non sicure

ESEMPIO:
1.Avvio CD/DVD
2.Avvio USB
3.Avvio SSD
In questo esempio basterà inserire un DVD o una USB e il LIVE si avvierà.
ESEMPIO:
1.Avvio SSD
2.Avvio USB/CD/DVD
Anche questo esempio potrebbe sembrare sicuro in un primo momento ma anche questo esempio risulta essere non sicuro in quanto l'ssd può essere bypassato non solo tramite BIOS modificando la sequenza bensì semplicemente togliendo l'SSD dal vostro PC, e non essendo rilevato andrà a fare il boot della periferica successiva.

Un altro tipo di attacco è l'attacco Evil Maid, in pratica si tratta di compromettere il vostro dispositivo cambiando il bootloader(in sostanza la schermata dove inserite la password con VeraCrypt) mettendone uno loro che salva la password da qualche parte e permette poi in un secondo momento alle FDO di accedere.
Gli attacchi Evil Maid sono attacchi per Target importanti solitamente, possono essere veicolati tramite dispositivi esterni che vengono collegati al vostro PC o tramite reti.
In questo caso essere sicuri che le FDO non siano connesse alla vostra Rete Lan interna e non vi connettiate a WiFi pubblici che potrebbero veicolare tale tipo di attacco.
L'attacco può essere posto in essere anche dopo un sequestro del vostro pc, poi restituito. In questo caso per recuperare i dati all'interno ricordatevi di isolare

completamente la macchina (wifi/lan ecc..), accendete il computer e recuperate i file di cui avete bisogno, successivamente formattate tutto completamente, e poi crittografate nuovamente. In modo che nel caso di un secondo sequestro l'attacco evil maid non abbia successo. Nel caso non abbiate bisogno dei file, procedete alla formattazione direttamente senza accedere al PC stesso e poi procedete nuovamente a crittografare il disco.

VeraCrypt permette la verifica delle firme del Bootloader in modo da capire se è stato compromesso o meno per un attacco Evil Maid, vi avvertirà direttamente all'avvio dello stesso (E' consigliato comunque la formattazione e la reinstallazione di VeraCrypt in caso le forze dell'ordine abbiano avuto in mano il PC)

TELEFONO CELLULARE
Che telefono utilizzare?

La risposta migliore è non utilizzare un telefono.
Ma se volete utilizzare un telefono cosa scegliere tra un Android o un iOS ?

La scelta corretta in questo caso è utilizzare un dispositivo della Apple.
Per estrapolare i dati da un dispositivo mobile viene utilizzato prevalentemente il software UFED DI Cellebrite.

Perchè scegliere iOS rispetto ad Android?

Le ultime versioni di Android in accoppiata agli ultimi modelli di telefoni sono sicuri, però questa sicurezza è effimera, in quanto UFED viene aggiornato frequentemente con nuovi exploit per Android ogni 1-2 mesi. Purtroppo se vi sequestrano il telefono non andranno a fare la perizia immediatamente, bensì l'accertamento tecnico irripetibile verrà fatto almeno 6 mesi dopo il sequestro dello stesso, e a quel punto i vostri dati verranno estrapolati. Inoltre molte marche ricevono le patch di sicurezza in ritardo oppure smettono di riceverle dopo poco tempo.
I dispositivi Apple invece hanno un tempo di sicurezza maggiore, e quindi quando verrà fatto l'accertamento tecnico non ripetibile, i vostri dati potrebbero con buona probabilità essere al sicuro.
Attualmente non esiste nessun Exploit per estrapolare i

dati da dispositivi con chip A12+ (quelli non supportati da checm8).

IMPRONTA E FaceID, SI o NO?

Sia l'impronta che il FaceID sono estremamente sicuri, allo spegnimento del dispositivo bisogna sempre inserire il codice d'accesso al telefono.
Il codice di accesso deve essere necessariamente superiore a 10 cifre, sennò si potrebbe essere soggetti ad un attacco BruteForce.

Attenzione:
Se le forze dell'ordine recupereranno il vostro codice d'accesso potranno cambiare il volto su FaceID e/o le impronte, e quindi anche le app protette potranno essere sbloccate.

Cosa utilizzare allora?
Il mio consiglio è di utilizzare esclusivamente il codice di blocco senza utilizzare FaceID e di utilizzare codici di blocco aggiuntivi (ovviamente diversi) per le app singole. Nel caso vogliate essere poco più comodi utilizzare FaceID o TouchID solo per l'autenticazione al telefono e non anche per l'accesso alle applicazioni.

iCloud?

La sincronizzazione di iCloud va disattivata completamente, ogni dato ad esempio contatti, note, backup, immagini sono accessibili dalle forze dell'ordine. Non dovete in nessun modo archiviare nulla su iCloud.

I TELEFONI VECCHIA SCUOLA SONO SICURI?

A differenza di quello che si è soliti credere i telefoni vecchia scuola, quali Nokia e simili non sono sicuri.

SIM FISICA O eSIM?

La SIM fisica può essere estratta dal telefono e diventare una prova, che vi può collegare al reato, mentre una eSIM risulta essere esclusivamente digitale e se il dispositivo è bloccato resterà lì.

PROVIDER EMAIL?

La maggior parte dei provider di email condivide le informazioni comprese le email stesse alle forze dell’ordine. I provider che potete utilizzare senza incorrere in questo rischio sono Protonmail e Tutanota che sono provider di mail crittografate. Entrambi i siti però salvano l’indirizzo IP dal quale una determinata persona si collega per leggere le email quindi dovrete prestare attenzione a questo dettaglio.
Utilizzate sempre caratteri generici per le vostre mail, non utilizzate mail o nickname che possano ricondurvi a voi.

VPN? PROXY?

Le VPN/Proxy permettono di camuffare il proprio indirizzo IP in modo che durante la navigazione né risulti uno diverso e molti provider di VPN/Proxy permettono anche la scelta della località.
I provider di VPN però salvano l'IP originale che si è collegato al loro servizio, in questo caso parliamo di VPN/Proxy che tengono i Logs (dati)
La differenza tra VPN e Proxy è che nella prima il traffico è cifrato mentre nella seconda il traffico non è cifrato ed è possibile intercettarlo.
Esistono però VPN che non salvano logs tra le quali è d'obbligo citare NordVPN e Mullvad.

VPS?

Molte persone non sanno che le forze dell’ordine possono accedere tranquillamente alle VPS con un decreto firmato dal giudice. Se voi utilizzate il vostro proprio IP per collegarvi alla VPS e poi commettete reati fraudolenti anche usando Proxy sarà molto facile per loro risalire al vostro indirizzo IP e quindi trovarvi.

IP di una SIM PRESTANOME?

Una SIM prestanome è una sim intestata a terzi. La SIM prestanome non permette però di avere la sicurezza che non veniate rintracciati, in primo luogo verrà chiamato a rispondere la persona intestataria del numero di telefono però poi quando si evincerà che la persona in questione non è la persona che ha commesso il reato, andranno più in fondo analizzando i tabulati telefonici e telematici.

TABULATI TELEFONICI E TELEMATICI

Molte persone credono che i tabulati telefonici vengono utilizzati esclusivamente per reati gravi.
Esiste un principio di proporzionalità che nega in via teorica l'uso dei tabulati per reati poco gravi, ma è un principio e nel caso il pm decida di procedere per questa via non c'è nessuna legge che glielo impedisca.
Per quanto vengono salvati i tabulati telefonici?
Secondo le ultime normative europee i tabulati devono essere conservati per 72 mesi(6 anni).
E comprendono i seguenti dati:
Cella Telefonica utilizzata (via dove è posizionata)
IMSI(numero chiamante)
IMSI(telefono che riceve chiamata)
IMEI del telefono utilizzato per la chiamata
DURATA CHIAMATA
I tabulati non contengono il contenuto degli sms o delle chiamate, se siete sotto osservazione però possono attivare le intercettazioni in modo che vedano e ascoltino le vostre chiamate e/o SMS.
Si può capire subito che sostituire semplicemente la SIM non è sufficiente nel caso siete osservati, perché l'IMEI del vostro dispositivo rimarrà lo stesso e potranno trovare facilmente la nuova sim che avete inserito nel telefono e quindi intercettarvi.
Le celle telefoniche però non permettono di avere al 100% precisione sulla posizione della sim. Potete digitare il pratico codice *3001#12345#* e sotto la voce "nbr_rsrp" potete vedere la potenza del segnale il dB.

Trovate una mappa sulla posizione delle celle sul sito:
https://www.opencellid.org/

Tabulati Telematici cosa sono?

Solitamente vengono impostati i DNS della compagnia telefonica di Default e tutte le query al DNS vengono salvate per 6 anni.

DNS CONSIGLIATI

I DNS consigliati sono quelli di Google (8.8.8.8) che cancellano i log ogni 48H.

Potete utilizzare la tecnologia DoH(DNS over HTTPS) in modo che le richieste siano crittografate e nessuno possa avere accesso ad esse.

Per attivare DoH su Windows 10 dovrete aggiungere il seguente valore al registro:

Nella seguente cartella

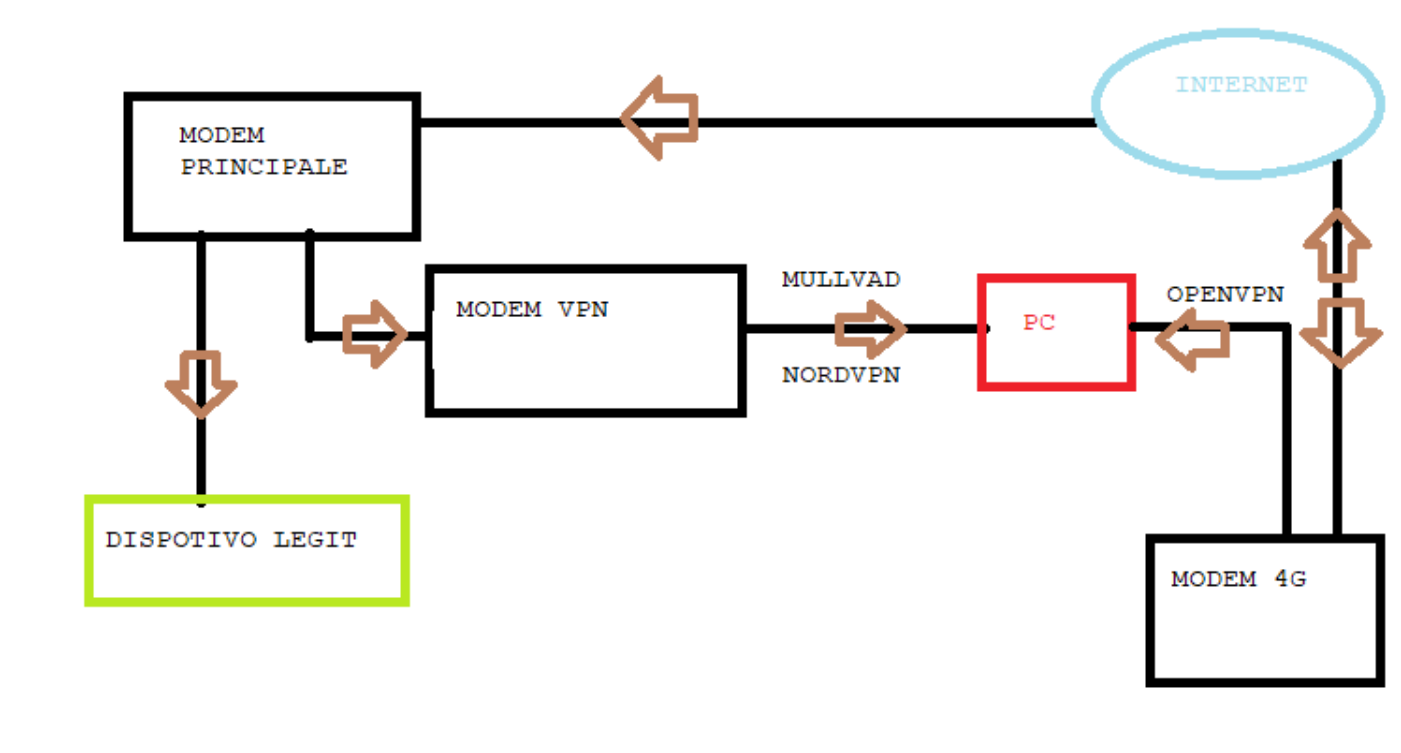
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters`

Aggiungete un valore DWORD a 32bit nominato

EnableAutoDoh e con valore 2 (Esadecimale)

SETUP IDEALE

Per evitare che le forze dell'ordine riescano a rintracciare il vostro IP e di conseguenza arrestarvi consiglio il seguente setup in modo che possiate dormire sogni tranquilli.



IL PC o il Telefono saranno connessi al Modem che si collegherà direttamente al provider della vostra VPN consiglio il gl.inet mango dal costo veramente contenuto (appena 20€) che ha sia wifi sia una porta Ethernet. Successivamente vi collegherete al modem 4g

posizionato lontano da voi dove avrete avviato openvpn server. In questo modo potrete avere l'ip della sim 4G.
Attenzione: Non tornate mai a controllare cosa è successo al vostro modem, potrebbero esserci le forze dell'ordine ad aspettarvi o aver posizionato una videocamera per identificarvi.

Dove posizionare il modem 4G?

Per migliore la propria opsec dovrete posizionare la sim e il modem 4G lontano da voi, è fortemente consigliato lasciare il modem vicino alla persona di cui assumerete l'identità falsa. In modo che nel caso di indagini avrete sempre un capro espiatorio.
Quante identità false?
Per avere una buona opsec dovrete avere almeno 3-4 identità false.
Avere un identità falsa significa avere una mail documenti conti e sim tutto collegato tra di loro, in modo che nel caso di problemi vadano a prendere la persona in questione e al 90% la processeranno e la dichiareranno colpevole, mentre voi sarete liberi.

TELEGRAM E’ SICURO?

Telegram è abbastanza sicuro poiché non condivide le informazioni con le forze dell’ordine. Telegram condivide informazioni con le forze dell’ordine nel caso il vostro account venga utilizzato per fare propaganda terroristica o contenga pedopornografia salvata sulle chat. Quindi se non avete materiale del genere telegram è ottimo per i reati comuni. La crittografia end-to-end di Telegram permette lo scambio anche dei materiali sopra indicati senza che ve ne sia traccia sul vostro account. In questo modo telegram non condivide nulla e voi state sicuri.
Come fa Telegram a riconoscere tale materiale? Le forze dell’ordine condividono con telegram gli hash dei file, telegram scansiona la presenza degli stessi e nel caso di esito positivo condivide le informazioni da loro richieste.
ATTENZIONE alle chiamate peer to peer, condividono il vostro ip direttamente con l’altra persona, fate passare tutto per i server di telegram.

WHATSAPP E’ SICURO?

Whatsapp come telegram ha la crittografia end to end però loro condividono l’ultimo ip di connessione, la vostra rubrica e hanno in casi gravi un sistema per cambiare in remoto la chiave per la crittografia, quindi

automaticamente avendo la chiave possono leggere le conversazioni.
Discord/Instagram e simili collaborano con la polizia, statene alla larga.

METADATA E FILE

Ogni foto che scattate contiene alcuni dati come posizione dove la avete scattata e informazioni sul dispositivo utilizzato per scattarla. Questi metadata possono essere cancellati, ci sono app come telegram o whatsapp che le cancellano in automatico però altre non sono così, quindi attenzione. Cercate di non scattare foto del posto dove vi trovare degli oggetti che vi circondano, di voi, e non condividete alcun dato su di voi neanche generico.
Le forze dell'ordine sono riusciti a trovare un pedofilo grazie all'angolazione della luce in una foto e un particolare fiore. Anche il codice seriale di un prodotto al supermercato potrebbe fregarvi, quindi niente foto.
Non raccontate nulla a nessuno anche se fidato, che conoscete da anni. Ognuna di queste cose potrebbe compromettere la tua opsec. La cosa migliore da fare è mantenere sempre un profilo molto basso.

CARDING, TRUFFE, ESTORSIONI

Questi tipi di reati sono i più comuni online, la polizia non segue le traccie informatiche in questo caso bensì la merce e/o denaro. Poiché è più facile da seguire e si arriva più velocemente a chi ha commesso il reato.

INDIRIZZO DI COMODO(DROP)

Per chi fa carding (acquisto di oggetti con carte di credito altrui) è necessario avere un drop. Il drop è il primo posto dove andranno in caso di perquisizione, quindi è fortemente sconsigliato utilizzare casa di un amico o di un vicino.
La polizia potrebbe mettersi a fare appostamenti cercando di identificare chi prende il pacco. E' consigliato cambiare il drop ogni tot tempo.
Potete mandare a prendere ad un altra persona il pacco e poi consegnarvelo, però nel caso questa persona venga fermata dalla polizia dovete assicurarvi che non si metta a collaborare con loro (non potete mai avere la certezza). Anche lasciare il pacco in un luogo indicato potrebbe portare la polizia a fare accertamenti sul luogo d'incontro con il negro che vi è andato a prendere il pacco per portarvelo.
Per truffe e/o estorsioni è comodo avere un posto dove mandare soldi, il prelievo al bancomat è facilmente traccaibile.

Il BITCOIN E' TRACCIABILE?

SI, un wallet non corrisponde a un identità tranne però è possibile tracciare dove vanno i soldi perché la blockchain(una sorta di libro mastro con tutte le transazioni) è pubblica, dunque consultabile da tutti.

SE LA POLIZIA VI TROVA?

La polizia potrebbe beccarvi in flagranza di reato, ad esempio mentre state vendendo la dose al vostro cliente, lì non c'è niente da fare, vi arresterà e dovrete fare il processo.
In italia al primo reato non si va mai in carcere perché esiste l'attenuazione per la tenuità del reato, insomma se il reato non è grave vi fare i domiciliari o qualcosa di socialmente utile e via.
Se il giudice invece ha qualche sospetto su di voi potrebbe firmare una perquisizione domiciliare. Nei casi normali 3 agenti vengono a sorpresa a casa dalle 7 alle 20 e sequestrano tutto il materiale pertinente al reato. Se è la polizia e il reato è informatico vi basterà spegnere tutto (tenete una ciabatta con interruttore vicino) e non sarà più possibile accedere a nulla. Nel caso di reati più gravi potrebbero entrare irrompendo in casa anche da finestre (non sto scherzando) in quel caso la presa con interruttore è fondamentale. Diventa fondamentale anche dell'acido dove buttare materiale compromettente.
Attenzione:Quando andate a posizionare le vostre cose all'esterno state attenti a telecamere e a lasciare impronte digitali. Esistono telecamere wireless con durata batteria annuale che potete mettere sul luogo d'interesse e controllare in remoto.

A cosa fare attenzione durante la perquisizione?

Nelle classiche perquisizioni gli agenti guardano dove state guardando voi, e questo vi frega se avete

nascosto qualcosa. Sguardo perso nel vuoto da strabico è la soluzione.
Dovete fare anche molta attenzione alle cimici che vi possono mettere a casa durante la perquisizione (molto più frequente di quanto immaginiate), quindi dopo una perquisizione non dite niente ad alta voce a nessuno, non parlate tra di voi e non andate subito nel vostro nascondiglio a spostare le cose che non hanno trovato.
Se avete la possibilità comprate un rilevatore di giunzioni non lineari, serve per trovare silicio e metallo,utilizzatelo per bonificare l'ambiente e vedere se ci sono microspie.
I modelli che vi consiglio sono EDD-24T oppure quelli della cayman.
Un semplice rilevatore di frequenze non è sufficiente perché esistono cimici antibonifica o spente che non possono essere rilavate, mentre un rilevatore di giunzioni non lineari riesce a trovare anche una sim dentro un libro.
Attenzione esistono anche microfoni direzionali e microfoni laser che permettono l'ascolto di conversazioni anche a distanza senza che abbiano posizionato nulla, e nel caso di microfoni laser anche attraverso finestre.
Dovete stare attenti anche ad appostamenti di poliziotti in borghese che vi seguono.

E SE LA SITUAZIONE E' CRITICA?

In caso la situazione sia troppo critica, avete l'ultima opzione quella di andare in un paese senza estradizione verso l'Italia. E' più consigliato andare in paese del terzo mondo dove grazie alla corruzione e pochi soldi (per loro tanti) potrete avere documenti nuovi e identità nuova e farvi una vita da liberi.

DISPOSIZIONI DA PARTE DELLE PROCURE SU COME INDAGARE PER REATI DI TIPO INFORMATICI / TRUFFE

Disposizioni da parte delle Procure su come indagare per Reati di tipo informatici / truffe. Qui sotto posto direttamente copia integrale dal Leak senza che stia a riscrivere. Un grazie al Procuratore della repubblica che ha redatto il tutto e a me stesso per averlo leakato.Nelle pagine seguenti viene spiegato in modo dettagliato comprensivo di qualificazione giuridica del reato, descrizione del fenomeno, elementi che l'ufficiale di PG(polizia giudiziaria) deve acquisire e gli accertamenti per raccogliere la notizia criminis.

I - PARTE GENERALE

1. Verifica preliminare della condizione di procedibilità e possibilità legittima di presentare una mera denuncia (in luogo di una querela)

La maggior parte dei reati informatici è procedibile a querela di parte[2], e dunque l'acquisizione della stessa, nelle forme previste dalla legge costituisce una condizione di procedibilità. Solo la querela (e non anche la mera denuncia) è considerata condizione di procedibilità dal momento che, tramite la stessa, la persona offesa manifesta esplicitamente la volontà che si proceda in ordine al fatto reato di cui è vittima (art. 336 c.p.p.).

Data la corretta informazione al cittadino, è auspicabile verificare la possibilità che possa bastare la semplice denuncia laddove l'intento non sia quello di far iniziare un procedimento penale ma solo quello, come spesso capita nella materia che qui interessa, di disconoscere la riferibilità a sé stesso: di una determinata casella *e-mail;* di un determinato account di *Facebook* e/o di altro social network o sistema di comunicazione (es. *chat);* di determinate spese delle carte di debito/credito o telefoniche.

Per questa ragione è da evitare il ricorso a modelli prestampati, recanti a priori l'intestazione con la denominazione "*denuncia/querela*", ovvero caselle precompilate da validare con un mero frego. **La volontà di proporre una querela** (e non una semplice denuncia), come la volontà di essere informati in caso di presentazione di richiesta di archiviazione e/o di proroga delle indagini, deve essere verificata caso per caso, sondando il reale intendimento del soggetto che si presenta.

2. Importanza delle informazioni da richiedere in sede di denuncia o di querela

La persona offesa/danneggiata dal reato è normalmente in grado di fornire utili elementi di prova (anche di natura informatica). In questo caso è necessaria la loro corretta acquisizione prima di ogni altra valutazione ai fini del prosieguo delle indagini[3].

---

[2] Sono perseguibili a querela di parte le seguenti fattispecie: art. **595 c.p.** – Diffamazione; **art. 612 comma 1 c.p.** – Minaccia (ove quindi non sussistano le circostanze aggravanti di cui al comma 2); **art. 612 bis commi 1 e 2 c.p.** – Atti persecutori (ove quindi non sussistano le circostanze aggravanti di cui al comma 4); **art. 612 ter comma 5 c.p.** – Diffusione illecita di immagini o video sessualmente espliciti (ove quindi non sussistano le circostanze aggravanti di cui al comma 4 o il fatto non sia connesso con altro delitto per il quale si debba procedere d'ufficio); **art. 615-ter comma 1 c.p.** – Accesso abusivo ad un sistema informatico o telematico (ove quindi non sussistano le circostanze aggravanti di cui ai commi 2 e 3); **art. 617-quater commi 1 e 2 c.p.** – Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (ove quindi non sussistano le circostanze aggravanti di cui al comma 4); **art. 635-bis comma 1 c.p.** – Danneggiamento di informazioni, dati e programmi informatici (ove quindi non sussistano le circostanze aggravanti di cui al comma 2); **art. 640 comma 1 c.p.** – Truffa (ove quindi non sussistano le circostanze aggravanti di cui al comma 2 o altre circostanze aggravanti, quali quelle di cui all'art. 61 c.p.); **art 640 ter comma 1 c.p.** – Frode informatica (ove quindi non sussistano le circostanze aggravanti di cui al comma 2 o altre circostanze aggravanti, quali quelle di cui all'art. 61 c.p.

[3] E così ove si debba acquisire una pagina web o un intero sito, occorrerà seguire le indicazioni riportate nell'approfondimento tecnico.

In termini generali (fatti salvi gli approfondimenti per ciascuna tipologia di reato di seguito riportati), vengono qui indicati alcuni elementi di fatto che dovrebbero essere forniti dalla persona offesa o, comunque, alla stessa richiesti laddove intenda proporre non già una mera denuncia, ma una querela:

- *siti web:* nome del sito; stampa delle pagine, se il sito non è pedopornografico (se contiene immagini di minori è sufficiente il nome della pagina web);
- *messaggi presenti in newsgroup, blog, etc.:* indicazione del nome del *newsgroup* e del modo di poterlo individuare sulla rete; stampa del messaggio, se questo non è pedo-pornografico (se contiene immagini di minori è sufficiente spiegare come poterlo reperire);
- *social network (Facebook, Twitter, Instagram, ecc.):* nome del *social network* adoperato; giorno e ora dell'attività segnalata; ID *(Identification Number)* dell'utente; ID del gruppo; URL[4] completo del profilo; indirizzi *e-mail* rilevati; stampa del profilo; sunto delle conversazioni avviate all'interno del *social network*;
- *e-mail:* copia dell'email ricevuta comprensiva dell'*header*[5] (intestazione del messaggio nella sua forma estesa) del messaggio e degli allegati (anche se sono relativi a immagini pedo-pornografiche);
- *chat:* giorno e ora della *chat*; nome della *chat* adoperata; *nick name* proprio e dell'utente con cui si è conversato; dati della stanza in cui è avvenuta la conversazione; testo della conversazione; *log* relativi alla conversazione in *chat*; *file* inviati durante la *chat*;

3. I dati del traffico telematico (*File di log*[6])

Per la conservazione dei dati del traffico telefonico e telematico per "*finalità di accertamento e repressione dei reati*" l'attuale norma di riferimento è l'art. 132 del D.lgs. 196/2003 (Codice Privacy). Tale norma prevede che, per i dati attinenti al traffico telefonico (cd. tabulati) e le chiamate senza risposta, il periodo di conservazione sia, rispettivamente, di 24 mesi e di 30 giorni, mentre per i dati attinenti al traffico informatico (cd. *File di log*) il periodo di conservazione è fissato in 12 mesi. Per risalire all'utilizzatore di una determinata connessione internet, gli operatori di Polizia Giudiziaria possono contare sul fatto che la macchina (*server)* in uso al fornitore del servizio (es. Telecom, Vodafone, etc.) conserva i relativi *files* di *log,* ovvero quelli che il nostro legislatore chiama "*dati relativi al traffico telematico*", generati da quell'evento[7].

Come per i tabulati, anche per i file di log è necessario un provvedimento di acquisizione del Pubblico Ministero, da notificare al gestore interessato. In caso di richieste di log all'Autorità Giudiziaria, sarà allegato quale ultima pagina anche un foglio che riproduce i dati da richiedere, contenente i seguenti dati:

IP: *81.12.140.50 specificando sempre il fornitore (provider) – es. Telecom*

---

[4] Un Uniform Resource Locator o URL è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in Internet, come un documento o un'immagine (es. www.giustizia.it)

[5] Intestazione di un messaggio di posta elettronica, che indica il mittente, il luogo, l'ora di spedizione e altre informazioni per l'instradamento del messaggio fra i server Internet, tra cui l'indirizzo IP utilizzato.

[6] Nella lingua inglese il termine log indica il diario di bordo di una nave, ma viene applicato estensivamente anche ad altri veicoli e macchine tra cui il computer. Nel gergo informatico, "loggare" (da verbo inglese to log) significa registrare all'esito di una attività di monitoraggio. E, quindi, il log file (o file di log) è il risultato di tale operazione, che assume la forma di un file (di testo) nel quale vengono appunto indicate le operazioni che l'utente compie durante la sua sessione di lavoro, anche su internet.

[7] Così come, alla stessa stregua, per risalire all'utilizzatore di una determinata utenza cellulare è possibile acquisire - tramite estrapolazione dalle apparecchiature in uso al relativo gestore - i dati del traffico telefonico, a tutti noti come i c.d. tabulati.

Data: *01/01/2017 prestando attenzione al formato (Europeo o Americano)*
Fascia Oraria: *dalle ___ alle ____ (chiedere un intervallo di tempo congruo rispetto all'evento informatico di interesse, prestando attenzione all'ora legale/solare. Nel caso di connessione NAT[8] invece l'orario deve essere preciso al secondo)*
Fuso Orario: *es. CET (Italia) o PST (USA California) – (spesso i gestori esteri come Google o Facebook forniscono i file di log con fuso orario americano che va convertito o specificato in decreto)*

Con l'approvazione del decreto legge nr. 225 del 29.12.2010 si è proceduto all'abrogazione delle disposizioni che disciplinano l'identificazione degli utenti, il monitoraggio delle operazioni e l'archiviazione dei dati presso gli Internet Point, i *phone center* e chi offre accessi liberi alla Wi-Fi. Pertanto, non è più possibile risalire agli utilizzatori delle postazioni Internet in tali siti.
Con il decreto legislativo n.101 del 10 agosto 2018, infine, è stato introdotto all'interno dell'art.132 Codice della Privacy, il comma 5-bis che contiene un rinvio all'art. 24 della Legge n. 167 (Legge Europea) del 20 novembre 2017, di adeguamento della disciplina nazionale alla Direttiva Comunitaria nr. 2017/541 sulla lotta al terrorismo, secondo cui, per soddisfare l'esigenza di contrasto del terrorismo a livello internazionale, **i dati di traffico telefonico e telematico vanno conservati non più per 1 ma per 6 anni[9]**.
Quanto finora indicato vale per gli "*operatori*" italiani (ai sensi dell'art. 1 lett. c del Codice delle Comunicazioni Elettroniche). Le società estere, che ugualmente offrono a cittadini italiani "*servizi di comunicazione elettronica accessibili al pubblico*", ritengono di non dover essere assoggettate alla normativa italiana (di derivazione comunitaria) in materia di obblighi di conservazione dei dati relativi al traffico telematico. E dunque, da esse (si pensi a Facebook, Google, Microsoft e Yahoo) sarà possibile ottenere informazioni - di regola - relative agli ultimi 45/60 giorni, fino, in alcuni casi, ad un massimo di 90 giorni (es. Facebook, anche se tale periodo di tempo non viene "*garantito*", così come del resto l'invio dei dati completi).
Come per i gestori italiani, per le richieste di *file* di *log* sarà di regola sufficiente il provvedimento del Pubblico Ministero. Nelle richieste ai gestori stranieri così come nelle loro risposte, occorre ricordare come sia fondamentale precisare il **fuso orario di riferimento.**
Per le **richieste di intercettazioni di comunicazioni e per i contenuti di profili o caselle di posta elettronica** è, allo stato, necessario approntare una apposita richiesta di

---

[8] Nell'ambito delle reti informatiche, il network address translation (abbreviato in NAT) è un meccanismo che permette di modificare l'indirizzo IP dei pacchetti in transito attraverso apparati di rete – come router o firewall – all'interno di una comunicazione in corso tra due o più nodi della rete. Il meccanismo del NAT è diventato fondamentale nel momento in cui gli indirizzi IP del protocollo IPv4 hanno cominciato a scarseggiare. L'aumento esponenziale dei dispositivi connessi alla Rete ha fatto sì che gli indirizzi disponibili in questo spazio di rete (4 miliardi e 300 milioni circa) si esaurissero in fretta. Il NAT è stato quindi utilizzato per poter nascondere dietro un unico indirizzo pubblico decine e decine di indirizzi privati (e quindi altrettanti device). Nonostante l'introduzione del protocollo IPv6, questa tattica di "*mascheramento*" degli indirizzi privati è molto utilizzata sia per semplice comodità sia perché capace di garantire un certo numero di vantaggi.

[9] Art. 24. Termini di conservazione dei dati di traffico telefonico e telematico: 1. In attuazione dell'articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'articolo 4-bis, commi 1 e 2, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, è stabilito in settantadue mesi, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-bis, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

commissione rogatoria.
È importante ricordare come **i maggiori operatori telefonici italiani** (Vodafone, Fastweb, Wind/Tre, Telecom, Iliad, ecc.) **e i maggiori Social Network** (Facebook, Instagram, Whatsapp, Twitter, Google, Microsoft, etc.) abbiano messo a disposizione della Polizia Giudiziaria piattaforme informatiche e/o PEC per gli accertamenti relativi a intestatari sim/account Internet, tabulati telefonici e file di log, come meglio descritto nella parte dedicata all'approfondimento tecnico.

4. Modalità di conseguimento del profitto illecito - Primi accertamenti

Molto spesso gli accertamenti di tipo tecnico informatico, che saranno illustrati nel dettaglio più avanti nella parte dedicata all'approfondimento tecnico, risultano impossibili alla luce delle informazioni raccolte in sede di denuncia/querela. Vi sono, invece, altri approfondimenti esperibili che non presentano difficoltà di natura tecnica e che possono essere eseguiti direttamente dalla Polizia Giudiziaria che ha ricevuto la querela, conseguendo validi risultati: in tutti questi casi l'attività investigativa da intraprendere deve essere indirizzata verso accertamenti di tipo "*tradizionale*", finalizzati a reperire riscontri oggettivi utili per l'individuazione del beneficiario finale del trasferimento delle somme di denaro.
In relazione alle truffe online, di regola, il profitto illecito viene indirizzato su **carte di credito prepagate (ricaricabili)**. Per le carte postepay occorrerà contattare Poste italiane, mentre per le altre carte ricaricabili occorrerà individuare e contattare di volta in volta l'istituto di credito emittente. Poste Italiane ha messo a disposizione delle Forze dell'Ordine un sistema, denominato *PosteAG*, per interrogazioni online e in tempo reale sugli intestatari dei conti correnti e delle carte prepagate di Poste Italiane.
Per commettere le truffe online viene anche adoperato lo strumento del **vaglia postale e online**.

- Il vaglia postale ordinario dà la possibilità di inviare denaro a un'altra persona, da qualsiasi ufficio postale, senza necessità di essere titolari di conto corrente postale o bancario, previa compilazione in una filiale di Poste, del relativo modulo di richiesta. L'operatore rilascia il numero del vaglia che il mittente provvederà a comunicare al beneficiario insieme alla parola chiave (composta da un minimo di tre fino a un massimo di sedici caratteri) e all'importo.
- Il vaglia online può essere disposto solamente dai correntisti di Poste Italiane mediante la compilazione dell'apposito modulo presente nel sito Internet della società Poste Italiane. Si differenzia da quello ordinario per la sua possibile riscossione in tempo reale in qualsiasi ufficio postale previa fornitura della parola chiave prevista per l'operazione.

Spesso nelle condotte illecite viene utilizzato il servizio cd. di **money transfer** che permette di trasferire, da persona a persona, il denaro da una parte all'altra del mondo nel giro di pochi minuti. In Italia i maggiori operatori sono rappresentati dagli agenti Western Union (www.westernunion.com) e Money Gram (www.moneygram.com) e proprio questi, per la loro contestuale presenza in quasi tutti i paesi del mondo, vengono indicati - in via esclusiva - nelle e-mail dirette ai *financial manager* o nei messaggi volti a ottenere il trasferimento di una somma di denaro come prezzo di un bene che tuttavia non verrà

mai recapitato. In tale tipo di operazioni assume notevole importanza il codice MTCN (Money Transfer Control Number), che consente di identificare in maniera univoca l'operazione effettuata. Normalmente le società di trasferimento di denaro (money transfer) richiedono gli estremi del documento di identità presentato per effettuare l'operazione, senza però trattenerne la fotocopia. Ne consegue che quando il denaro è inviato all'estero non è possibile effettuare ulteriori accertamenti, e ricorrere allo strumento della rogatoria sarebbe inutilmente dispendioso.

Capita sempre più spesso che siano utilizzati, come parte del meccanismo fraudolento, degli **assegni**, già intestati, inviati quale forma di pagamento anticipato, spesso del valore maggiorato rispetto all'importo del bene da acquistare. Il venditore attende che l'importo del titolo sia accreditato sul suo conto in banca prima di effettuare l'operazione e trasferisce le somme di denaro secondo le modalità pattuite. Trattandosi di assegni esteri, gli istituti di credito non danno immediati riscontri sulla falsità degli assegni. Altra truffa molto diffusa si basa sul porre all'incasso assegni circolari (soprattutto postali) inviati precedentemente dal truffatore via email o whatsapp (per testimoniare l'interessamento all'acquisto di un bene), quindi stampati e riscossi prima dell'appuntamento in cui sarebbe dovuto avvenire lo scambio bene – assegno.

Si è verificato anche che il profitto illecito venga indirizzato su **conti correnti bancari**. In questi casi sarà comunque immediatamente possibile risalire all'istituto di credito interessato laddove sia indicato dalla persona offesa il codice IBAN di tale istituto beneficiario. L'IBAN[10] è un codice composto da 27 caratteri che identifica in modo univoco un conto corrente. Di recente l'IBAN è risultato anche associato non a un conto corrente bancario, ma a una carta di credito ricaricabile (tipo postepay), il che contribuisce a trarre in inganno i truffati. Tramite numerosissimi siti internet è possibile identificare la filiale di appartenenza di un determinato conto corrente (del quale si è in possesso del numero IBAN o, comunque, almeno del numero ABI e CAB). Di regola identificare l'esatta filiale interessata rileva, oltre che per l'identificazione concreta del beneficiario, anche ai fini della competenza territoriale.

Molto spesso possiamo trovarci di fronte a denunce querele che indicano come conti correnti beneficiari quelli di Fineco Bank, Banca Medialanum, WeBank, IWBank, INGDirect o N26, ossia di istituti di credito privi di sportelli sul territorio (e, infatti, proprio per tali motivi, si parla di **banche online**). Con alcune importanti conseguenze sotto il profilo dell'individuazione della competenza territoriale. Il *locus commissi delicti* non può, infatti, identificarsi *ipso facto* nella sede legale della banca. Sarà fondamentale l'analisi della movimentazione bancaria che - previa richiesta di un idoneo provvedimento di acquisizione a opera del Pubblico Ministero ex art. 256 c.p.p. - consentirà alla Polizia Giudiziaria di verificare il luogo (normalmente coincidente con quello della residenza/domicilio) ove le somme accreditate siano state effettivamente poste all'incasso.

II - LE TIPOLOGIE DI REATO E GLI ACCERTAMENTI MINIMI RICHIESTI

Alcuni dei reati informatici che di seguito saranno analizzati non rientrano nelle previsioni della legge 48/2008 e, quindi occorrerà trasmetterli alle Procure Circondariali secondo i

[10] International Bank Account Number.

criteri generali di competenza: in particolare non sono reati distrettuali le seguenti ipotesi: **furto di identità**: 494 c.p.; **truffa e-bay o su altra piattaforma informatica**: art. 640 c.p.; **riciclaggio elettronico proventi illeciti** (*cyber laundering*): artt. 648, 648 bis c.p.; **carte di credito**: art. 493 ter c.p. (salve le ipotesi ex art. 617 quinquies c.p. - installazione di apparecchiature atte ad intercettare la comunicazione intercorrente tra il *chip* della carta di credito e il sistema informatico dell'istituto di credito - o ex art. 615-quater c.p. laddove con tale condotta – di regola accompagnata anche dalla acquisizione, tramite meccanismi di videoripresa, dei relativi codici PIN all'atto della loro digitazione - abusivamente l'agente si procura codici di accesso al sistema informatico della banca); **diffamazione online**: art. 595 comma 3 c.p..

Furto d'identità

Qualificazione giuridica

Art. 494 c.p. - Sostituzione di persona (competenza non distrettuale)

Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica con la reclusione fino a un anno[11].

Fenomeno

Trattasi di un fenomeno variegato, ricomprendente:

A) tutti i tentativi di *phishing* tramite invio di e-mail, es. quelle che sembrano provenire da noti istituti di credito (Poste Italiane, MPS, etc.). In questo caso la più corretta qualificazione giuridica appare essere quella di cui agli artt. 56, 494, 640-ter c.p.;

B) altri furti di identità, anche consumati, che nella maggior parte dei casi si concretizzano con l'attivazione di schede telefoniche, conti correnti on-line, sottoscrizione di finanziamenti, profili social.

Elementi da acquisire in denuncia

Giorno in cui si è avuta contezza del furto di identità e quant'altro si ritenga utile; copia dell'eventuale documentazione relativa l'attivazione del servizio a proprio nome e successivamente disconosciuto; estremi dei numeri identificativi del servizio attivato (ID o nickname profilo Facebook, email, account Ebay, etc.); documentazione relativa all'attività illecita compiuta (eventuali messaggi o post pubblicati, immagini o video diffusi, etc.).

Accertamenti minimi richiesti

Nel caso sub A) l'attività risulta di fatto preclusa e potrà essere trasmessa una CNR tra i

---

[11] Cass. Sez. 5. Sentenza n. 46674 del 08/11/2007 Ud. (dep. 14/12/2007) in CED 238504: "*Integra il reato di sostituzione di persona (art. 494 cod. pen.), la condotta di colui che crei ed utilizzi un "account" di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete 'internet' nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese, subdolamente incluso in una corrispondenza idonea a lederne l'immagine e la dignità (nella specie a seguito dell'iniziativa dell'imputato, la persona offesa si ritrovò a ricevere telefonate da uomini che le chiedevano incontri a scopo sessuale)*".

"*procedimenti seriali*" da produrre mensilmente, con l'indicazione che non vi è ulteriore attività di indagine da svolgere, salvi i casi di particolare rilievo.

Nel caso sub B)

- Occorrerà accertare innanzitutto se tale ipotesi ha causato un effettivo danno.
- Occorrerà verificare - chiedendo innanzitutto alla persona offesa - cosa è stato fatto in concreto con i propri dati.
- In caso di disconoscimento di una identità da parte di una determinata persona, verrà verificato se sussistono precedenti denunce di smarrimento dei relativi documenti di identificazione o se la stessa ha presentato denunce in relazione all'invio sulla rete internet (per vari motivi) dei suoi documenti.
- Si potrà verificare nel caso di schede telefoniche come e in quale località si procede alla loro ricarica o dove le stesse siano state attivate presso il gestore competente.
- Per i conti sarà opportuno verificare la movimentazione di conto (anche attraverso decreto dell'A.G. competente) e se vi sono ritiri di contante tramite sportello bancomat avente data recente (di norma non superiore a 7 giorni), richiedere le immagini della videoregistrazione dopo aver contattato l'Istituto bancario interessato.

Pregresse esperienze investigative

Sub A) Gli accertamenti di tipo tecnico informatico sugli illeciti riconducibili al fenomeno del "*phishing*" risultano spesso impossibili perché i link relativi ai siti clone, presenti all'interno della mail, di regola sono visualizzabili per breve tempo.

Se tali dati vengono acquisiti, le verifiche di solito non forniscono elementi utili per l'identificazione dell'autore dei reati posti in essere, in quanto si è visto in pregresse indagini che l'invio dei messaggi avviene dall'estero o che l'ubicazione delle macchine ospitanti i siti web clone è estera. In altri casi le macchine che vengono usate sono già violate o senza protezioni. Tali circostanze non permettono di svolgere ulteriori attività investigative senza il ricorso a una rogatoria internazionale, il cui esito, anche se potenzialmente positivo, comunque difficilmente consentirebbe di giungere all'individuazione dei responsabili della frode.

Violazione account

Qualificazione giuridica

Art. 494 c.p. - Sostituzione di persona – vedi sopra

Art. 615-ter c.p. - Accesso abusivo ad un sistema informatico o telematico (competenza distrettuale)

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

Art. 615-quater c.p. - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (competenza distrettuale)

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è

punito con la reclusione sino a un anno e con la multa sino a euro 5.164.

art. 616 c.p. - Violazione, sottrazione e soppressione di corrispondenza (competenza non distrettuale)

Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prender cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da euro 30 a euro 516. ..... Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica o telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.

Fenomeno

Trattasi di un fenomeno più complesso rispetto al precedente, ricomprendente varie ipotesi
A) Violazione account eBay o di altre piattaforme di commercio elettronico (o di bacheche annunci vendita), al fine di porre fittiziamente in vendita su Internet - avvalendosi di una identità non corrispondente al reale venditore - beni con l'intento di non inviarli all'acquirente, così ottenendo l'ingiusto profitto del prezzo che di regola viene corrisposto tramite pagamenti elettronici prima dell'invio del bene. Di tale fenomeno l'utente (che ha subito la violazione del proprio account) ne viene a conoscenza a seguito della comunicazione che lo stesso si vede recapitare dagli Istituti di recupero crediti di transazioni online.
B) Violazione/acquisizione indebita dell'account personale/profilo Facebook o di quello relativo ad altre piattaforme di social network o dell'account di posta elettronica, messo in atto al fine di contattare in maniera dissimulata altri utenti dello stesso social network, ovvero per creare azioni di disturbo o molestia o diffamazione.

Elementi da acquisire in denuncia

nome dell'account violato e il giorno in cui si è avuta cognizione della sottrazione dell'account; indicazione di tutte le persone che sono legittimamente a conoscenza delle credenziali di accesso; indicazione di eventuali situazioni personali e/o professionali che potrebbero giustificare la violazione dell'account; descrizione dell'attività illecita posta in essere con l'account sottratto (esempio: invio email, molestie, diffamazione): l'eventuale ripresa di possesso dell'account, e in caso positivo far fornire al denunciante i log relativi agli ultimi accessi, di norma direttamente recuperabili all'interno dell'account stesso; in caso di comunicazioni a opera di istituti di recupero credito o delle società titolari dei servizi attivati, la persona offesa dovrà allegarne copia: la persona offesa dovrà allegare anche tutte le informazioni utili attestanti l'avvenuta violazione dell'account; indicare le persone che conoscevano la password o che avrebbero potuto conoscerla (per prossimità o frequentazione con l'utente): luogo di consultazione dell'account/casella di posta elettronica, tipo di collegamento usato; modalità di percezione dell'utilizzo indebito della casella/periodo temporale nel quale la casella è stata violata; contenuto della casella al momento dei fatti della violazione, con particolare riferimento alla presenza di messaggi di grande rilevanza.

Accertamenti minimi richiesti

Nel caso in cui si fosse in possesso dei log di accesso fraudolenti verificare se gli IP di connessione siano esteri o italiani: 1) nella prima ipotesi sarà sufficiente trasmettere la notizia di reato alla Procura competente, rappresentando l'impossibilità di continuare l'attività di indagine sul territorio nazionale; 2) nel secondo caso sarà sufficiente trasmettere la notizia di reato alla Procura competente, richiedendo un decreto di acquisizione file di log da notificare al gestore competente. La Procura provvederà a delegare l'attività tecnica ritenuta necessaria.

Come nel caso di furto di identità semplice (cfr. sopra), occorrerà verificare se tale ipotesi ha causato un effettivo danno alla persona offesa.

Bisognerà specificare se si tratti di violazione di un account/profilo già esistente o se invece è stato creato *ex novo* un account/profilo: in questo caso la parte lesa dovrà indicare gli aspetti specifici di riconducibilità di tale account/profilo alla sua persona (per escludere, per esempio, che si tratti di mera omonimia).

In caso di accesso abusivo a server aziendali, la stessa persona offesa può acquisire - anche a mezzo di consulente tecnico di parte - e trasmettere alla Polizia Giudiziaria, anche a integrazione dell'originaria denuncia querela, i file di log registrati nei relativi sistemi informatici.

Occorre, infine, richiedere alla persona offesa se la casella di posta elettronica è abbinata ad altri servizi o conti correnti online, invitandola a provvedere al più presto al cambio del riferimento e-mail per tali servizi.

Pregresse esperienze investigative

Nel caso sub A) l'acquisizione fraudolenta dell'*account* spesso avviene con tecniche di *social engineering*[12], tramite invio di *e-mail* che inducono il legittimo titolare a rivelare a terzi (che, solo apparentemente, sono ricollegabili ai gestori della piattaforma elettronica) i dati relativi al proprio *account.* L'esperienza investigativa acquisita in analoghi casi ha consentito di determinare come tali azioni, se non giustificate da motivi personali o professionali, di regola provengono da persone che, operando dall'estero, si avvalgono di tecniche informatiche idonee al mascheramento della propria identità. Anche un'eventuale richiesta di assistenza giudiziaria, mediante rogatoria, porterebbe a esiti negativi, considerato peraltro i limitati termini di conservazione dei dati informatici.

Nel caso sub B) trattasi di un'ipotesi specifica rispetto a quella precedente. Non sempre la persona offesa ha prova dell'utilizzo indebito dell'account, e con esso, del realizzarsi del furto di identità ex art. 494 c.p..

Con specifico riferimento all'email spesso la persona offesa si limita a denunciare un mero malfunzionamento della casella di posta elettronica o non è in grado di indicare alcuna

---

[12] Il social engineering riunisce una serie di tecniche rivolte a spingere le persone a fornire informazioni personali come password o dati bancari o a consentire l'accesso a un computer al fine di installare segretamente software dannosi. I ladri e i truffatori utilizzano il social engineering in quanto è più facile spingere una persona a rivelare le proprie password rispetto all'ottenere tali informazioni mediante tecniche da hacker. Sono molte le tecniche utilizzate dagli esperti di social engineering. Tra queste, vi è il *baiting* (offrire qualcosa al fine di consentire il download di un file dannoso), il *phishing* (una mail realizzata appositamente per favorire l'inserimento di informazioni personali), il *pretexting* (l'impersonare qualcuno per ottenere l'accesso a dati privilegiati) o lo *scareware* (spingere l'utente a credere che il proprio computer sia infetto per poi offrire una soluzione con cui infettarlo veramente).

altra particolare circostanza di fatto che possa far ricollegare l'episodio denunciato a una (ipotetica) intrusione ad opera di terzi, tale da consentirne una presa di conoscenza dei messaggi ivi presenti e/o un utilizzo indebito.
Si è peraltro rilevato che molto spesso l'atto è presentato unicamente per disconoscere eventuali attività effettuate con la casella a titolo precauzionale o per dichiararsi estranei alla divulgazione di contenuti relativi a messaggi inviati, senza l'effettiva intenzione di individuare il responsabile degli abusi: in tal caso, l'interessato dovrà essere informato della possibilità di **presentare una mera denuncia**.

Altro accesso abusivo: attacchi mediante inoculazione di virus

Qualificazione giuridica

Art. 615-ter c.p. - Accesso abusivo ad un sistema informatico o telematico – vedi sopra

Art. 615-quater c.p. - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici – vedi sopra

Art. 615-quinquies c.p. - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (competenza distrettuale)

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici(2), è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

Fenomeno

Trattasi di vere e proprie intrusioni informatiche mediante lo sfruttamento di vulnerabilità di sistema (bug) finalizzate alla diffusione di virus che consentono all'autore del reato (hacker) di prendere possesso del computer infetto per gli scopi più disparati, normalmente di natura economica.
Molto ricorrenti sono gli attacchi informatici realizzati attraverso i *trojan ransomware*[13], che sono un tipo di cyberware progettati per estorcere denaro. I metodi di installazione più comuni del *trojan ransomware* sono: tramite e-mail di *phishing* o tramite l'accesso a un sito Web contenente un programma nocivo.

Elementi da acquisire in denuncia

Giorno in cui si è avuta cognizione della violazione del sistema informatico; indicazione di tutte le persone che sono legittimamente a conoscenza delle credenziali di accesso; indicazione di eventuali situazioni personali e/o professionali che potrebbero giustificare la violazione del sistema; descrizione delle attività illecite poste in essere (esempio: invio email, creazione di false pagine di istituti di credito, blocco del computer o della rete, etc.);

[13] Dopo che è stato installato, il trojan crittografa le informazioni memorizzate sul computer della vittima oppure impedisce il normale funzionamento del computer, lasciando anche un messaggio con una richiesta di pagamento per decrittografare i file o ripristinare il sistema. Nella maggior parte dei casi, la richiesta di riscatto appare quando l'utente riavvia il computer dopo l'avvenuta infezione.

l'eventuale ripresa di possesso del sistema e, in caso positivo, far fornire al denunciante i log relativi agli ultimi accessi di norma direttamente recuperabili dall'amministratore di sistema; se si tratta di sistema aziendale, la persona che potrà presentare denuncia deve essere l'Amministratore delegato della predetta azienda, ovvero l'Amministratore di rete della stessa che deve premunirsi di una relazione tecnica dell'amministratore di sistema dell'azienda; copia dell'email ricevuta comprensiva dell'*header* (intestazione del messaggio nella sua forma estesa) del messaggio e degli allegati.

Accertamenti minimi richiesti

La stessa persona offesa può acquisire – anche a mezzo di consulente tecnico di parte – e trasmettere alla Polizia Giudiziaria, anche a integrazione della originaria denuncia querela, informazioni sull'accesso abusivo subito, fornendo i file di log.

La Polizia Giudiziaria dovrà verificare il luogo di ubicazione dei server interessati dalla condotta di accesso abusivo, circostanza rilevante al fine della **competenza territoriale**[14].

Nel caso in cui si fosse in possesso dei log di accesso fraudolenti verificare se gli Ip di connessione siano esteri o italiani: 1) nella prima ipotesi sarà sufficiente trasmettere la notizia di reato alla Procura competente, rappresentando l'impossibilità di continuare l'attività di indagine sul territorio nazionale; 2) nel secondo caso sarà sufficiente trasmettere la notizia di reato alla Procura competente, richiedendo un decreto di acquisizione file di log da notificare al gestore competente. La Procura provvederà a delegare l'attività tecnica ritenuta necessaria.

Pregresse esperienze investigative

L'esperienza investigativa acquisita in analoghi casi ha consentito di determinare come tali azioni, se non giustificate da motivi personali o professionali, di regola provengono da persone che, operando dall'estero, si avvalgono di tecniche informatiche idonee al mascheramento della propria identità. Anche un'eventuale richiesta di assistenza giudiziaria, mediante rogatoria, porterebbe a esiti negativi, considerato peraltro i limitati termini di conservazione dei dati informatici.

Estorsioni online

Qualificazione giuridica

Art. 629 c.p. - Estorsione (competenza non distrettuale)

Chiunque, mediante violenza o minaccia, costringendo taluno a fare o ad omettere qualche cosa, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da cinque a dieci anni e con la multa da euro 1.000 a euro 4.000.

Fenomeno

La parola "*sextortion*" è un neologismo inglese nato dalla crasi tra sex ed extortion (sesso ed estorsione). Indica un ricatto sessuale realizzato attraverso il web. Si tratta di una pratica usata da cyber criminali per estorcere denaro alle vittime. Ne esistono tre varianti.

---

[14] Il Procuratore Generale presso la Corte di cassazione, con provvedimento del 17 maggio 2010, così motivata sul punto: "*...sembra incontestabile, pur nella difficoltà di attribuire una precisa localizzazione alle diverse fasi del processo informatico e in assenza di precedenti in sede di legittimità, che il luogo ove si determina l'accesso al sistema non è quello nel quale si verifica l'azione volta a produrre questo risultato e nemmeno quello dal quale opera il soggetto titolare del diritto di escludere. Sembra che il luogo fisico ove si concentrano tanto le misure volte a tutelare il diritto di escludere quanto le informazioni che si intendono tutelare è quello ove si trova il server. Nell'ipotesi che esso non sia noto o che si trovi al di fuori del territorio dello Stato subentreranno i criteri residuali*".

A) variante classica: le persone prese di mira ricevono un invito o una richiesta di amicizia tramite le reti sociali (p.es. su Facebook o su una piattaforma di *dating*) da parte di una persona molto attraente a loro sconosciuta. Una volta accettato l'invito o la richiesta, la persona in questione inizia a chattare con il soggetto preso di mira. Durante la conversazione, le propone poi di passare a una videochat (per es. in Skype) e cerca di convincerla a spogliarsi, masturbarsi, o assumere pose indecenti. Per raggiungere il proprio scopo, inganna la sua vittima, dicendole di trovarla molto attraente, di sentirsi eccitata sessualmente da lei e/o di non avere nessuna inibizione nei confronti della nudità e della masturbazione. Per apparire credibile, compie il primo passo scoprendo per esempio il seno o fingendo di masturbarsi davanti alla webcam. Tutte le azioni che la persona presa di mira compie davanti alla webcam durante la videochat sono registrate a sua insaputa. In seguito, la vittima è contattata da ricattatori che la esortano a pagare, minacciandola di mettere tutto quanto ripreso su YouTube a suo nome, di inviare questo materiale sensibile per e-mail a familiari, amici o datori di lavoro, oppure di pubblicare il link su Facebook;
B) variante SPAM[15] ***(fake sextortion)***: capita anche che i tentativi di ricatto qui sopra descritti siano inviati a moltissime persone come e-mail di spam contenente una «*minaccia infondata*». Gli *spammer* sperano di individuare fra i vari destinatari persone che hanno recentemente guardato film o immagini porno e si augurano che la minaccia inviata li spaventi al punto da indurli a pagare. In questi casi, il computer delle vittime non è infettato e in realtà gli *spammer* non sono affatto in possesso di materiale compromettente;
C) variante *malware*: in questa forma di sextortion, i computer, i tablet e gli smartphone di persone che navigano in siti con contenuti pornografici sono infettati da un *malware*. Questo software dannoso attiva la webcam che riprende la vittima a sua insaputa mentre guarda film o immagini porno. Le riprese spesso compromettenti sono quindi trasmesse ai pirati informatici che poi ricattano la vittima, minacciandola di pubblicare il materiale sensibile o di inviarlo alla sua lista di contatti, anch'essa rubata.

Elementi da acquisire in denuncia

Estremi dei numeri identificativi dell'account/profilo dell'estorsore (ID o nickname profilo Facebook, email, ecc.); documentazione relativa all'attività illecita compiuta (eventuali messaggi o post pubblicati, immagini o video diffusi, etc.); copia dell'email ricevuta comprensiva dell'*header* (intestazione del messaggio nella sua forma estesa) del messaggio e degli allegati: mezzo di pagamento utilizzato per pagare l'estorsore.

Accertamenti minimi richiesti

La *sex extortion* è un fenomeno crescente e si presenta sotto due fenomenologie: una tipicamente domestica, spesso riconducibile a coppie che si separano, con uno dei due (quello che la subisce) che diffonde sul web immagini intime dell'ex partner, l'altra, a dimensione internazionale, dettata esclusivamente da ragioni di profitto, in cui tra attore e vittima non esiste alcun legame, e gli autori sono quasi sempre localizzati all'estero (Africa o Asia).
Nel primo caso, la Polizia Giudiziaria provvederà a identificare l'account/profilo dell'estorsore, fornendo all'ufficio legale di contatto del gestore del servizio (es. Social

[15] Lo spam (o spamming) indica l'invio anche verso indirizzi generici, non verificati o sconosciuti, di messaggi ripetuti ad alta frequenza o a carattere di monotematicità tale da renderli indesiderati (generalmente commerciali o offensivi). Lo spam è noto anche come posta spazzatura (in inglese junk mail).[1] Può essere attuato attraverso qualunque sistema di comunicazione, ma il più usato è Internet, attraverso messaggi di posta elettronica, chat, tag board, forum, Facebook e altri servizi di rete sociale.

Network Facebook) il nome dell'utente e acquisendo così il *form* di registrazione dell'utente con i dati, comprensivo di indirizzo email, nonché l'indirizzo IP di connessione. Una volta ottenuti i log di accesso occorrerà verificare se gli IP di connessione siano esteri o italiani: 1) nella prima ipotesi sarà sufficiente trasmettere la notizia di reato alla Procura competente, rappresentando l'impossibilità di continuare l'attività di indagine sul territorio nazionale; 2) nel secondo caso, sarà sufficiente trasmettere la notizia di reato alla Procura competente, richiedendo un decreto di acquisizione file di log da notificare al gestore competente. La Procura provvederà a delegare l'attività tecnica ritenuta necessaria.

Pregresse esperienze investigative

L'esperienza investigativa acquisita in analoghi casi ha consentito di determinare come tali azioni, se non giustificate da motivi personali o professionali, di regola provengono da persone che, operando dall'estero, si avvalgono di tecniche informatiche idonee al mascheramento della propria identità. Anche un'eventuale richiesta di assistenza giudiziaria, mediante rogatoria, porterebbe a esiti negativi, considerato peraltro i limitati termini di conservazione dei dati informatici e che il pagamento spesso viene effettuato con bonifici o trasferimenti di denaro all'estero (prevalentemente Costa d'Avorio e altri paesi del continente africano).

Truffa su piattaforme di compravendita o siti e-commerce

Qualificazione giuridica

Art. 640 c.p. - Truffa (competenza non distrettuale)

Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

o **art. 640 comma 2 n.2 bis c.p. - Truffa aggravata dalla c.d. "minorata difesa**[16]"

La pena è della reclusione da uno a cinque anni e delle multa da euro 309 a euro 1549 .... 2 bis) se il fatto è commesso in presenza della circostanza di cui all'art. 61, numero 5.

Fenomeno

A) Gli utenti si accordano, tramite servizi di commercio *online* (in particolare eBay), per acquistare/vendere della merce. Dopo alcuni contatti via mail o via telefono, l'accordo viene raggiunto.

---

[16] Cass. Sez. II Pen. 14/10/2016 nr. 43705 - La Suprema Corte ha ritenuto che, in tema di compravendita in internet e quindi di contratto, il necessario equilibrio tra le parti contraenti viene ad alterarsi a causa delle peculiari caratteristiche e modalità di utilizzazione del mezzo telematico: così, in caso di mancata consegna del bene acquistato, si configura l'aggravante della "*minorata difesa*". L'art. 61 c.p., comma 1, n. 5, stabilisce che l'aggravante della cosiddetta minorata difesa si configura allorquando l'agente abbia approfittato di circostanze di tempo, di luogo o di persona, anche in riferimento all'età, tali da ostacolare la pubblica o privata difesa. A riguardo, va ricordato che, in genere, le circostanze di luogo e di tempo devono essere oggettivamente conosciute dall'agente e questi deve averne volontariamente approfittato: tale valutazione va effettuata in concreto, caso per caso e complessivamente in base agli elementi disponibili (Cass. Sez. II 07-01-2015 n. 13933, Sez. I 10-07-2013 n. 40923 e 16-05-2013 n. 13387), come uno stato di debolezza fisica o psichica, un furto o una rapina in ore notturne (Cass. Sez. V 26-01-2015 n. 32244), un reato commesso in luogo isolato od abbandonato (Cass. Sez. II 08-07-2004 n. 44624). Segnatamente, però, in caso di compravendita on line, tale approfittamento può presumersi: così, il luogo di consumazione del reato "*aggravato*" viene a coincidere con quello in cui si trova(va) l'agente nel momento in cui ha conseguito il profitto (Cass. Sez. II 04-11-2014 n. 7749). In altri termini, non è invocabile la volontaria esposizione, da parte del "*truffato*", al «*rischio*» del mezzo telematico quale concorso di colpa, non potendo infatti pretendersi una diligenza ad hoc da parte della persona offesa dal reato (Cass. Sez. II 25-09-2014 n. 42941 e 03-07-2009 n. 34059).

1) Se il truffatore è il venditore questi, una volta ricevuto il pagamento di quanto convenuto o un anticipo, fa perdere le tracce di sé non rispondendo più ai solleciti dell'acquirente.

2) Nel caso in cui il truffatore sia l'acquirente questi, a seguito di falsa email da parte del servizio Paypal o di un altro istituto bancario che certifica l'avvenuto pagamento, induce il venditore a spedire la merce (spesso all'estero). Solo dopo alcuni giorni, il venditore/truffato si accorgerà che il denaro non è mai stato accreditato e di aver perduto la merce. In altri casi, dopo aver raggiunto l'accordo sulla cifra, il compratore/truffatore fornisce dettagliate informazioni sul pagamento, invitando il venditore/truffato a recarsi presso uno sportello bancario. Quindi, con raggiri lo induce a effettuare una ricarica/bonifico in suo favore, mentre il venditore/truffato crede erroneamente di ricevere il pagamento.

B) Creazione di falsi siti di negozi *on line* finalizzati alla vendita truffaldina di merce di vario genere (per lo più di materiale elettronico).

In tutti i casi sopracitati le modalità di pagamento sono le seguenti: ricariche di carte di credito prepagate (ad esempio Postepay); bonifico bancario; trasferimento di denaro tramite Western Union/Money Gram; altri sistemi di pagamento elettronico (es. Paypal); utilizzo di assegni circolari falsi (molto spesso stranieri)[17].

Elementi da acquisire in denuncia

In caso di truffa sub A):

- tutti i dati relativi all'inserzione/annuncio di vendita (numero identificativo dell'annuncio, numero identificativo e/o nickname del venditore, email e numeri telefono del venditore, oggetto in questione, se l'annuncio sia ancora presente ovvero se ripresentato da parte di altro apparente venditore ma con gli stessi numeri e email di contatto) che è apparso sul portale di vendita (eBay, subito.it, Kijiji, ecc.),
- stampa, ovvero la copia digitale, delle email di contatto comprensive di *header* tra acquirente e venditore,
- mezzo di pagamento utilizzato per acquistare la merce, numero di conto corrente o carta di pagamento, ecc., dove è stato inviato il denaro, fornendo copia della documentazione relativa allo stesso.

In caso di truffa sub B):

- formato digitale o stampa della pagina internet completa, comprensivo di URL (vedasi allegato tecnico) dove l'oggetto è stato messo in vendita,
- indicazione dei dati relativi alla partita IVA/codice fiscale del venditore (ove reperibili dalla inserzione/annuncio o dal sito internet).

---

[17] Tale tipologia di truffa è inizialmente emersa soprattutto in relazione alla piattaforma di *secondamano.it*, le cui modalità sono peraltro segnalate agli utenti dal relativo sito. *Offerta di pagamento superiore al prezzo del bene venduto: La truffa comincia con la ricezione di una mail, da parte di un ipotetico acquirente, interessato al prodotto che vorresti vendere. Si tratta generalmente di un acquirente che vive all'estero e che ti pagherà con un assegno. Generalmente il presunto acquirente ha molta fretta di acquistare l'oggetto e dice di avere un contatto in Italia che verrà a prendere il prodotto dove preferisci. In certi casi potrebbe offrirti due o tre volte la cifra da te richiesta a garanzia, e che potrai restituirgli la differenza alla ricezione del bene. Altre volte, potrebbe tentare di convincerti che l'assegno che ti invierà ha un importo maggiore perché parte di esso serve a sbrigare pratiche doganali o cose del genere. Quello che invece è certo è che se il bene, ad esempio, costa 2.000 euro e il presunto acquirente ti invia un assegno da 6.000 euro, ti chiederà senz'altro di inviargli la differenza. Attenzione perché la banca può accettare l'assegno e impiegare settimane prima di comunicarti che invece non è regolare e che tu hai inviato denaro a un'organizzazione criminale. Altre truffe simili nascono dall'utilizzo di ricevute di bonifico online falsificate o in caso di venditori che raccomandano un servizio di deposito a garanzia sconosciuto.*

- indicazione degli elementi che fanno presupporre la truffa e, segnatamente, gli artifizi e raggiri posti in essere dal sedicente venditore per conseguire l'ingiusto profitto, ovvero la serialità delle condotte sopra descritte, che sostanziano il reato distinguendolo dal semplice inadempimento di natura civilistica.

Accertamenti minimi richiesti

Caso sub A) nr. 1

Una volta acquisito il nome del portale di vendita, fornendo all'ufficio legale di contatto il nome del venditore (o il nickname) e il numero dell'annuncio, bisognerà:

- acquisire il *form* di registrazione con i dati, comprensivo di indirizzo email, nonché l'indirizzo IP di connessione,
- acquisire l'indirizzo IP di inserimento dell'annuncio,
- individuare i mezzi di accredito o di pagamento utilizzati dal venditore.

A questo punto, i nominativi forniti dal portale o meglio quelli derivanti dalla titolarità della carta di credito o del conto dove vengono versate le somme dovranno essere verificati con accertamenti anagrafici e alla banche dati delle forze dell'ordine.

Caso sub A) nr. 2

Richiedere i dati di registrazione dell'acquirente procedendo di seguito come sopra per il nr.1, e verificare l'email o il numero di telefono di contatto con il venditore in buona fede.

Caso sub B)

- verificare il nominativo del titolare del conto corrente o della carta di credito dove sono confluiti i soldi profitto della truffa, chiedendo tutte le informazioni all'istituto bancario o postale emittente,
- verificare i contatti telefonici ed email inseriti nel sito web nonché il nominativo che ha registrato il dominio,
- verificare l'intestatario del nome a dominio (sito web) tramite alcuni servizi online.

Ai fini della **competenza territoriale**, occorrerà poi verificare il luogo di effettuazione del pagamento da parte della persona offesa e il luogo di destinazione del pagamento, raccogliendo dalla persona offesa tutti i dati utili alla successiva compiuta identificazione del truffatore[18].

Infine, la Polizia Giudiziaria dovrà verificare subito, tramite richieste agli istituti di credito interessati, l'eventuale giacenza del profitto illecito e in caso positivo:

1) il responsabile dell'Istituto di credito verrà invitato a valutare l'opportunità di bloccare – autonomamente – tali somme (in attesa delle determinazioni della AG),

2) la Polizia Giudiziaria segnalerà tempestivamente alla AG tale circostanza richiedendo

---

[18] Il Procuratore Generale presso la Corte di Cassazione a partire dal 2008 ha precisato che nei casi di truffa commesso tramite **ricarica di carta Postepay** il luogo di consumazione del reato deve ritenersi quello in cui ha sede l'ufficio postale presso il quale viene compiuta l'operazione di ricarica di una carta ricaricabile, giacché in quel luogo e in quel momento si verifica la *deminutio patrimonii* del soggetto passivo, con contestuale arricchimento da parte dell'agente, arricchimento costituito dalla mera disponibilità e non già dall'effettivo utilizzo della somma profitto de reato (Cassazione Sezione Seconda Penale – Sentenza del 15 febbraio 2017, nr. 7294). Lo stesso Procuratore Generale presso la Corte di Cassazione è intervenuto per individuare la regola di competenza nel diverso caso di pagamento effettuato dalla persona offesa tramite **bonifico bancario** a favore del conto corrente del venditore. Con provvedimento del 29.10.2009 ha affermato che in tali casi "*l'effettivo conseguimento dell'ingiusto profitto da parte degli agenti con conseguente concreta e definitiva perdita del bene subita dalla parte offesa è avvenuto soltanto [...] con l'accreditamento della somma e il positivo esito del disposto bonifico bancario sul c/o predetto [...] (e quindi con modalità di tempo e di luogo diverse - agli effetti della definitiva diminuzione patrimoniale subita dal soggetto passivo e dell'incremento economico ingiusto acquisito dal soggetto attivo - da quelle seguite con il pagamento effettuato con la ricarica delle carte prepagate)*". In tali ipotesi quindi si ritorna ad applicare i criteri tradizionalmente seguiti da molte Procure già prima del 2005, criteri che meglio riescono a soddisfare esigenze di "concentrazione" di episodi delittuosi relativi allo stesso autore in capo ad un unico organo investigativo (prima che giudicante).

il sequestro o provvederà direttamente al sequestro preventivo, a seconda dei casi.

Pregresse esperienze investigative

Occorrerà verificare se si tratta di episodi seriali o posti in essere con artifizi e raggiri, poiché solo in tali casi i fatti possono assumere una rilevanza penalistica, dal momento che il semplice mancato ricevimento della merce (acquistata su Internet) integra una questione di natura civilistica.

Nel caso sub A), dall'esperienza investigativa maturata, si è rilevato che nella maggior parte delle ipotesi le connessioni a internet usate per commettere gli illeciti vengono effettuate a partire da PC in precedenza violati (cd. macchine "*bucate*" o "*zombie*") o da postazioni presenti all'estero, oppure sfruttando reti WIFI aperte, o, infine, attraverso connessioni mobili tramite SIM intestate a persone inesistenti.

Di poca utilità è anche l'attività di acquisizione dei tabulati telefonici, considerato che nella quasi totalità dei casi si tratta di utenze VOIP (SIM utilizzate per effettuare chiamate tramite internet senza quindi possibilità di poter individuare una cella di riferimento) o utenze usate esclusivamente per contattare le vittime. Pertanto, non è vantaggioso sviluppare le predette informazioni mediante decreti del Pubblico Ministero.

Ad ogni modo, la risoluzione degli indirizzi IP potrà essere richiesta ai vari gestori solo tramite apposito decreto emesso dal Pubblico Ministero.

Risulta più vantaggioso sviluppare l'attività investigativa seguendo il flusso di denaro, come descritto in precedenza sopra nel paragrafo "*Modalità di conseguimento del profitto illecito*".

Quanto al fenomeno sub B), trattandosi di condotte criminose commesse di regola dall'estero, i relativi accertamenti investigativi saranno di difficile esecuzione se non con ricorso a collaborazioni di Polizia Giudiziaria di differenti Stati e/o richieste rogatoriali.

In caso di truffa seriale, verrà altresì valutata l'opportunità di segnalare l'attività di commercio *online* alla Guardia di Finanza per la parte tributaria (in relazione anche al totale delle somme incassate).

Bonifico disconosciuto su altro conto (phishing[19])

Qualificazione giuridica

art. 640-ter c.p. - Frode informatica (competenza distrettuale) – vedi sopra

art. 648 c.p. – Ricettazione[20]

Fuori dei casi di concorso nel reato, chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque

---

[19] Il termine *"phishing"* indica un'attività fraudolenta in genere perfezionata sulla rete Internet, che consiste nella predisposizione di tecniche idonee a carpire fraudolentemente dati personali sensibili (quelli più di interesse sono le numerazione di carte di credito, i conti correnti online, i codici relativi a depositi effettuati in banca ed i pin dei bancomat, ovvero informazioni che per essere ottenute richiedono anche l'involontaria ma incauta collaborazione della vittima). L'autore dell'attacco di phishing si limita ad inviare ad un numero elevato di utenti della Rete un elemento di stimolo, che in genere consiste in un messaggio di posta elettronica o di un virus informatico, sperando nel ritorno di dati sensibili (user-id e password) da parte delle vittime, così da accedere al loro conto corrente bancario o postale. Con l'invio del messaggio di posta elettronica, l'intenzione dei truffatori è quella di far visualizzare il sito relativo al link inserito nell'e-mail, ovvero una pagina web clone dell'istituto di credito gestita dai criminali, ove l'utente viene invogliato ad inserire le proprie credenziali di accesso, così acquisite per gli usi illeciti. Cliccando sul link proposto, infatti, la pagina che viene caricata non è quella della banca, dell'istituto o della società corretta, ma quella di un sito web creato ad arto per consentire ai criminali di sottrarre e memorizzare le informazioni fornite da utenti ignari.

[20] La ricettazione si ritiene avvenuta nel luogo dove il denaro di provenienza delittuosa è stato ricevuto o o accreditato. E, peraltro, la più recente giurisprudenza consente perfino di configurare la più grave ipotesi di riciclaggio (Cass. , sez. VI, sent n. 43534 del 24 aprile 2012, depositata il 9 novembre 2012, rv 253798; Cass. sez II, sent. n. 546 del 7 gennaio 2011, dep. L'11 gennaio 2011, rv 249445; Cass. sez II, sent. 1422 del 14 dicembre 2012, depositata l'11 gennaio 2013, rv. 254050).

si intromette nel farle acquistare, ricevere od occultare, è punito con la reclusione da due ad otto anni e con la multa da euro 516 a euro 10.329.

Fenomeno

In tali casi la persona offesa si lamenta della fraudolenta captazione - tramite tecniche di phishing - di informazioni e dati riservati relativi a conti correnti online, con conseguente prelievo di ingenti somme di denaro a opera di terzi, tramite operazioni online. Un'evoluzione del fenomeno ormai consolidato del "*Phishing*" è lo "*Smishing*[21]". Il nuovo *modus operandi*, che mira sempre all'acquisizione illecita di codici dispositivi, si sviluppa mediante l'invio a reali clienti di falsi SMS di servizio bancari, originati da utenze telefoniche apparentemente riconducibili agli istituti di credito[22], che porta le ignare vittime, convinte psicologicamente della bonarietà delle richieste, a rilasciare i dati di accesso e autenticazione dell'home banking. In particolare, nel messaggio sms ricevuto, è presente un link ipertestuale, a cui puntualmente la parte si collega per poi essere reindirizzata su una pagina dove è richiesto di inserire alcuni dati sensibili, e che successivamente risulterà non funzionale per la prosecuzione della procedura di accesso, facendo apparire un messaggio in cui l'utente viene avvisato che sarà a breve contattato da un operatore per la risoluzione dei problemi. In tal senso, effettivamente dopo pochi minuti la vittima riceve una chiamata dal numero verde in uso alla banca, dove l'operatore come già accennato motivando alcuni problemi riesce a farsi consegnare le chiavi di accesso e dispositivi del conto, utilizzandoli per operazioni fraudolente, quali bonifici bancari e/o pagamento, o ad accreditare un'ulteriore dispositivo mobile al conto in maniera da utilizzarlo successivamente, per prelievi cardless (prelievi di contanti presso ATM bancari effettuati tramite smartphone con lettura di un codice QR).

Elementi da acquisire in denuncia

Indicazione della filiale e del numero di conto corrente dal quale è stato prelevato il denaro; indicazione integrale dell'Iban di destinazione; dettaglio dei movimenti disconosciuti (file di log, data e ora, beneficiario dell'operazione, carta ricaricabile, ecc.); sarebbe opportuno acquisire anche informazioni relative ai sistemi di sicurezza del conto corrente del denunciante (esempio: sms *alert*, *token*, *password* temporanea); indicazione se prima delle spendite fraudolente sia stato ricevuto un messaggio di posta elettronica relativo al *phishing*; in caso positivo, *header* (intestazione) dell'e-mail di *phishing* e messaggio in formato elettronico.

Accertamenti minimi richiesti

Si approfondiranno gli accertamenti riguardo alle movimentazioni disconosciute dai denuncianti/querelanti di trasferimento fondi: 1) bonifici bancari su altri conti correnti; 2) ricariche di carte prepagate; 3) ricariche di sim-card di telefonia mobile; 4) pagamenti di

---

[21] La parola smishing deriva dall'unione di "SMS" (messaggio di testo) inviato tramite cellulare, e "phishing". Con il "phishing", venivano inviate e-mail fraudolente, nel cui corpo erano indicate informazioni e presenti collegamenti ipertestuali, ingannevoli per il destinatario, inducendolo a collegarsi al link che lo reindirizzava su una pagina fake della banca o di altra Società finanziaria, dove lo stesso inseriva informazioni sensibili per l'accesso e l'utilizzo del servizio home banking. Lo stesso avviene per lo smishing, che semplicemente si configura non sull'account di posta elettronica ma con il servizio SMS.

[22] un servizio internet denominato "*Alias*" fa comparire quale origine dell'SMS una denominazione numerica scelta a piacere dal mittente, che nel caso in questione riconduce alla Banca della parte offesa

utenze tramite siti internet che consentano pagamenti online.
La persona offesa dovrà fornire tutti gli elementi utili al prosieguo delle indagini, ed in particolare allegare l'estratto conto completo, dal quale risultino i dati precisi della destinazione finale delle somme di denaro.
Allo stato, gli importi di maggior valore si hanno in relazione ai bonifici bancari verso altri conti corrente. In tali casi, occorrerà:

1. verificare - partendo dalle indicazioni raccolte dalla persona offesa – l'effettiva destinazione del pagamento (anche tramite ricerca dell'IBAN, al fine di identificare l'ubicazione dell'istituto di credito interessato), raccogliendo tutti i dati utili alla identificazione del luogo dello stesso, rilevante altresì ai fini della competenza territoriale.
2. una volta identificato, si richiederà, quindi, all'istituto di credito interessato, se le somme indicate dalla persona offesa siano state prelevate e da chi; verranno altresì acquisiti, se presenti, i documenti esibiti per l'apertura del conto corrente (e se ne verificherà l'autenticità).

In caso di ricarica di carta prepagata, verrà richiesto all'istituto di credito emittente analoghe informazioni relative al titolare della stessa.
In entrambi i casi, la Polizia Giudiziaria dovrà verificare **subito**, tramite richieste agli istituti di credito interessati, l'eventuale giacenza del profitto illecito. In caso positivo:

- il responsabile dell'Istituto di credito verrà invitato a valutare l'opportunità di bloccare - autonomamente - tali somme (in attesa delle determinazioni della AG);
- la Polizia Giudiziaria segnalerà tempestivamente all'AG tale circostanza richiedendo il sequestro o provvederà direttamente a quello preventivo, a seconda dei casi.

In caso di ricarica sim-card, verrà rimessa all'AG la valutazione sulle richieste ai gestori relativa agli intestatari, dal momento che siffatti accertamenti di regola hanno dato risultati negativi. Invero, sovente si tratta di schede *sim* fittiziamente intestate.
Si rappresenta che solo nel caso di dirottamento verso conti esteri di ingenti somme (sopra 10.000,00 euro) il Servizio di Polizia delle Comunicazioni, allertato dal Compartimento territorialmente competente, potrà interessare il collaterale organo di Polizia estera al fine di bloccare e ristornare le somme prelevate fraudolentemente, previa comunicazione e autorizzazione da parte del PM titolare del procedimento.

Pregresse esperienze investigative

Gli accertamenti di tipo tecnico informatico sugli illeciti riconducibili al fenomeno del "*phishing*" risultano spesso impossibili alla luce delle informazioni raccolte in sede di denuncia/querela poiché i link relativi ai siti clone, contenuti nell'e-mail, rimangono validi per breve tempo.
Se tali dati vengono acquisiti, le verifiche, anche se teoricamente perfezionabili, non forniscono elementi utili per l'identificazione dell'autore dei reati posti in essere, dato che si è accertato in pregresse indagini che l'invio dei messaggi avviene dall'estero, che l'ubicazione delle macchine ospitanti siti web clone è estera e che vengono usate strumenti già violati o senza protezioni. Tali circostanze non permettono di svolgere ulteriori attività investigative senza il ricorso a una rogatoria internazionale.
Vi sono, peraltro, altri approfondimenti esperibili che non presentano difficoltà di natura

tecnica e che possono essere eseguiti direttamente dalla Polizia Giudiziaria che ha raccolto la querela, conseguendo validi risultati: in tutti questi casi l'attività investigativa da intraprendere deve essere indirizzata verso accertamenti di tipo "*tradizionale*", risultando più vantaggioso seguire il flusso di denaro, come descritto in precedenza sopra nel paragrafo "*Modalità di conseguimento del profitto illecito*".

Frode "*man in the middle*" tramite accesso email

Qualificazione giuridica

art. 615-ter c.p. - Accesso abusivo ad un sistema informatico o telematico – vedi sopra

art. 615-quater c.p. - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici – vedi sopra

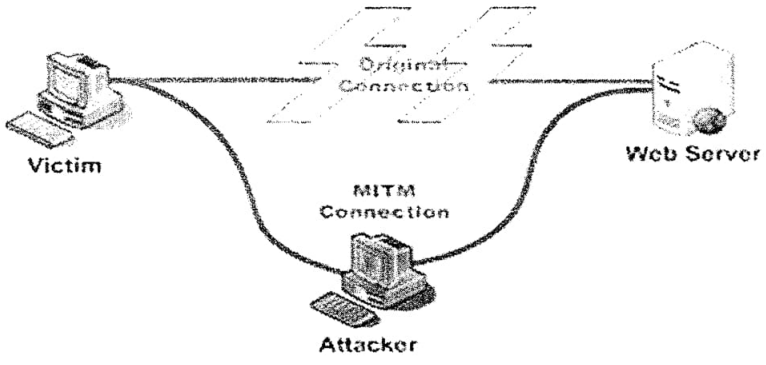
art. 616 c.p. - Violazione, sottrazione e soppressione di corrispondenza – vedi sopra

art. 617 sexies c.p. - Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (competenza distrettuale)

"Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni".

Fenomeno

L'*attacco dell'uomo in mezzo*, conosciuto anche con gli acronimi ***MITM*** o ***MIM***, è un tipo di attacco informatico con cui un soggetto non autorizzato, in gergo "*attaccante*", riesce a intromettersi nelle comunicazioni tra due parti con una modalità tale che nessuna di esse si accorga della compromissione del collegamento che le unisce reciprocamente, ma soprattutto con la possibilità di leggere i contenuti dei messaggi, nonché di inserirne o modificarne a piacere i contenuti, senza che nessuna delle due parti si renda conto dell'intromissione.



Il criminale prima carpisce informazioni sulle aziende attraverso la rete internet, sfruttando tecniche di *social engineering, insiders* aziendali, violando indirizzi e-mail, accedendo a *devices* aziendali smarriti o rubati, ecc., ma anche semplicemente (ma non solo) tramite visure camerali C.C.I.A.A..

Successivamente, approfittando di diversi fattori contingenti quali giorni di chiusura,

diverso fuso orario, ubicazione territoriale, lingue straniere che rendono difficoltosi sia i contatti in tempo reale che quelli telefonici (le aziende cinesi, ad esempio, si relazionano con quelle italiane esclusivamente a mezzo email), l'attaccante si sostituisce all'azienda "*x*" e si presenta alla ditta "*y*". Effettua, poi, ordinativi fraudolenti o finge di effettuare forniture attraverso pagamenti anticipati, oppure, nel caso di aziende con pregressi rapporti commerciali, comunica nuove coordinate bancarie per la ricezione di pagamenti di precedenti commesse ancora insolute.
Le false comunicazioni sono realizzate anche avvalendosi di indirizzi *email* appositamente creati che ricordano direttamente quelli dell'azienda presa di mira[23].
La prima *email* di comunicazione del cambio dei recapiti aziendali con quelli utilizzati per la frode avviene proprio attraverso l'indirizzo *email* reale dell'azienda violata, che viene utilizzato *una tantum* dal reo per rendere più credibile la truffa.

Elementi da acquisire in denuncia
Nome degli account violati e codice iban verso il quale è stato dirottato il denaro, mail originali ricevute da entrambi gli operatori economici, complete di *header*, dettagliata descrizione dell'evento, dettaglio delle operazioni di pagamento (normalmente tramite bonifico), e-mail comprensive di *header* utilizzate per realizzare la truffa, numeri di telefono relativi ai contatti intrattenuti con il truffatore, dati della reale e-mail del truffato, file di log della reale mail del truffato (per verificare eventuali accessi abusivi – tecnica social engineering).

Accertamenti minimi richiesti
Coinvolgere immediatamente il responsabile dei sistemi informatici dell'azienda vittima affinché vengano effettuate le verifiche di competenza e fornisca un quadro dettagliato (relazione tecnica) dell'evento ed impedisca che si protragga ad ulteriore conseguenze, coadiuvando al contempo gli operatori di P.G. nella raccolta dei dati necessari.
Nel caso in cui si fosse in possesso dei log di accesso fraudolenti alla casella di posta elettronica, verificare se gli Ip di connessione siano esteri o italiani.
Nella prima ipotesi, sarà sufficiente trasmettere la notizia di reato alla Procura competente, rappresentando l'impossibilità di continuare l'attività di indagine sul territorio nazionale.
Nel secondo caso, sarà sufficiente trasmettere la notizia di reato alla Procura competente, richiedendo un decreto di acquisizione file di log da notificare al gestore competente. La Procura provvederà a delegare l'attività tecnica ritenuta necessaria.
Qualora i legali rappresentanti delle aziende interessate non siano in grado di fornire dettagli tecnici relativi alle intrusioni informatiche subite, verranno invitati a contattare i propri amministratori di sistema al fine di estrapolare i dati richiesti.
Nel contempo andrà verificato l'intestatario del conto/carta ricaricabile ove è confluito il denaro; agli istituti di credito interessati andrà richiesto anche se a seguito della ricezione del denaro, sono avvenuti prelievi, giroconti o trasferimenti a vario titolo delle somme ricevute.
In entrambi i casi, la Polizia Giudiziaria dovrà verificare **subito**, tramite richieste agli

[23] Esempio: se l'indirizzo reale della società XYZ S.p.A. è info@societaXYZ.com, il criminale creerà l'indirizzo societaXYZ@gmail.com oppure, se l'indirizzo del direttore commerciale è antonio.rossi@societaXYZ.com, verrà creato antonio.rossi@yahoo.com..

istituti di credito interessati, l'eventuale giacenza del profitto illecito. In caso positivo:

- il responsabile dell'Istituto di credito verrà invitato a valutare l'opportunità di bloccare - autonomamente - tali somme (in attesa delle determinazioni della AG);
- la Polizia Giudiziaria segnalerà tempestivamente alla AG tale circostanza richiedendo il sequestro o provvederà direttamente al sequestro preventivo, a seconda dei casi.

Si rappresenta che solo nel caso di dirottamento verso conti esteri di ingenti somme (sopra 10.000,00 Euro) il Servizio di Polizia delle Comunicazioni, allertato dal Compartimento territorialmente competente, potrà interessare il collaterale organo di Polizia estera al fine di bloccare e ristornare le somme prelevate fraudolentemente, previa comunicazione e autorizzazione da parte del PM titolare del procedimento.

Pregresse esperienze investigative

È stato più volte accertato che gli intestatari dei conti utilizzati per ricevere il denaro sono dei personaggi marginali (*money mule*), utilizzati da organizzazioni criminali per monetizzare i proventi dell'attività illecita.

Tali nominativi possono comunque rivelarsi utili per dare inizio a specifiche attività di indagine.

Riciclaggio elettronico proventi illeciti (cyberlaundering)

Qualificazione giuridica

Art. 648 c.p. – Ricettazione – vedi sopra

Art. 648-bis c.p. - Riciclaggio (competenza non distrettuale)

Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000.

Fenomeno

Gli esiti delle indagini condotte in relazione al fenomeno del cd *phishing* che ha interessato numerosi istituti di credito italiani hanno evidenziato in alcuni casi che i proventi della predetta attività vengano inviati su conti correnti di soggetti che credono di svolgere un regolare lavoro. In questo caso, i co-autori del reato vengono contattati da fantomatiche società estere che a seguito della firma di un contratto di lavoro fittizio, si rendono disponibili a farsi recapitare merce (chiaramente acquistata con denaro fraudolentemente sottratto all'avente diritto) da controllare e poi rispedire all'estero, ovvero a farsi depositare somme di denaro sul proprio conto che successivamente preleveranno per poi spedirle con sistemi di pagamento, tipo Money Transfert, verso paesi esteri, che di fatto non consentono l'identificazione del beneficiario finale.

Tali bonifici online sono stati effettuati, in danno degli ignari titolari dei rispettivi conti ordinanti, previa illecita acquisizione delle rispettive credenziali (username e password, necessarie per le relative operazioni di home banking).

I titolari dei conti correnti italiani (cd. *Financial manager*) beneficiari di tali bonifici online, ritenendo di ottemperare a un contratto di lavoro, trattengono una percentuale di quanto a loro indebitamente accreditato e trasferiscono la residua somma a persone prevalentemente residenti nei paesi dell'Est Europa con le modalità sopra indicate.

Elementi da acquisire in denuncia

Diversamente dagli altri casi analizzati, la persona che denuncia il fenomeno è proprio quella che risulta essere coautore dell'ipotesi di reato. In tal caso, si può valutare l'ipotesi di acquisire la denuncia, valutando il deferimento all'A.G. in un momento successivo.

Per una migliore valutazione dell'attività di indagine da esperire si suggerisce la possibilità di prendere contatti diretti con il magistrato di turno.

Ad ogni modo, si effettuino le verifiche sulla disponibilità di somme ancora presenti sul conto di appoggio e la disponibilità del titolare a restituire le somme indebitamente ricevute. Ove si tratti di merce, si dovrà verificare se lo stesso è tuttora in possesso del materiale, procedendo al sequestro ai fini della restituzione agli aventi diritto.

Sempre più spesso, il *financial manager* si attiva con una denuncia/querela nei confronti di terzi, dopo aver saputo della provenienza illecita di alcune somme già ricevute (e ritrasferite all'estero). In siffatte ipotesi, dovranno quindi essere a lui richieste, oltre alle informazioni in suo possesso riguardo ai fatti (comprensive delle email ricevute dal sedicente "datore di lavoro"), anche le ricevute di trasferimenti all'estero già effettuati.

Verrà, altresì, chiesta la data e le modalità con le quali si è accorto dell'illiceità delle somme, al fine di verificare la sua buona o cattiva fede.

La Polizia Giudiziaria dovrà, altresì, accertare se il *financial manager* si sia adoperato per restituire la somma indebitamente ricevuta.

Verrà, infine, valutata l'opportunità di segnalare alla Guardia di Finanza eventuali contratti sottoscritti dal *financial manager*, per la parte tributaria (in relazione anche al totale delle somme dallo stesso incassate a titolo di provvigione).

Pregresse esperienze investigative

Quanto agli accertamenti idonei a identificare le persone operanti all'estero, dall'esperienza investigativa maturata si è rilevato che le connessioni a internet usate per attuare il richiamato *modus operandi* vengono effettuate a partire da macchine in precedenza violate o da postazioni situate all'estero; pertanto, non è vantaggioso sviluppare le predette informazioni mediante decreti del Pubblico Ministero, se non tramite OEI (ordine europeo d'indagine) o rogatoria internazionale.

Quanto alla condotta posta in essere dai beneficiari dei bonifici *online,* essa deve essere oggettivamente qualificata ai sensi dell'art. 648-bis c.p., essendo idonea a porre in essere una attività di riciclaggio di somme di denaro provento di reato (frode informatica, allo stato delle indagini commessa da soggetti tutti operanti all'estero). Ovvero ai sensi dell'art. 648 c.p. laddove, come verificatosi in alcuni casi, non sia avvenuto il successivo trasferimento dopo l'incasso.

La **competenza territoriale** si radica nel luogo nel quale tali somme sono state poste all'incasso, allo scopo di ritrasferirle all'estero (e dunque nel luogo ove è sito l'istituto di credito del *financial manager*) o comunque presso il luogo di residenza/domicilio ex art.

9 comma 2 c.p.p..

Carte credito

Qualificazione giuridica

art. 640-ter c.p. - Frode informatica (competenza distrettuale) – vedi sopra, **qualora il titolare non abbia perso il possesso della propria carta di pagamento**.

Art. 493 ter c.p. – (che ha sostituito l'art. 55 comma 9 D. Lvo 21 novembre 2007 nr. 231) **Indebito utilizzo e falsificazione di carte di credito e di pagamento** (competenza non distrettuale) - **nel caso in cui il titolare abbia perso il possesso della propria carta di pagamento**.

Chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

Fenomeno:

A) la persona offesa disconosce alcuni pagamenti effettati sul web, a sua insaputa, in quanto i codici della carta di credito vengono catturati fraudolentemente da ignoti mediante tecniche di hacking direttamente sul web; oppure la persona offesa disconosce dei pagamenti (acquisti presso negozi di vario genere) o dei prelievi effettuati su ATM (sportello bancomat), in quanto gli ignoti autori del reato hanno provveduto ad installare delle apparecchiature atte ad intercettare le comunicazioni tra il chip o la banda magnetica della carta e il sistema informatico dell'istituto di credito (esempio: installazione dello *skimmer*[24] sugli ATM dei vari istituti, quali Poste italiane, banche, etc.).

B) Sovente la Polizia Giudiziaria interviene nei pressi di istituti di credito o di sportelli bancomat. Solamente laddove gli indagati siano trovati nel materiale possesso di carte di credito sarà possibile l'arresto nella flagranza del reato.

Elementi da acquisire in denuncia

Sia nel caso A) che nel caso B)

- indicazione del numero della carta di debito/credito, del nome della società proprietaria e della banca emittente (possibilmente con l'indicazione della filiale e del relativo

[24] Lo *skimmer* è un dispositivo capace di leggere e in certi casi immagazzinare su una memoria EPROM o EEPROM i dati della banda magnetica dei badge. Le caratteristiche dello skimmer fanno sì che venga usato sempre più spesso per commettere attività criminose a danno dei titolari di carte di credito, degli utilizzatori degli sportelli Bancomat e dei distributori self-service di carburanti. In particolare sono due le fattispecie più comuni messe in pratica dai malfattori. La prima, la più nota, è messa in pratica dal malfattore che, approfittando del pagamento a mezzo carta di credito, effettua una copia dei dati contenuti nel badge a danno dell'ignaro titolare. La seconda, meno nota, avviene attraverso la clonazione del badge direttamente allo sportello Bancomat. Ciò avviene attraverso il posizionamento di uno skimmer, appositamente adattato, in corrispondenza della feritoia di inserimento della carta. Per la cattura del PIN, invece, è spesso impiegata una micro-telecamera nascosta che filma il codice digitato dall'utente. Alcuni malfattori utilizzano, in opzione alla micro-telecamera, una tastiera aggiuntiva posta sopra quella originale dello sportello che memorizza il PIN digitato.

numero di conto corrente);

- copia di estratto conto o lista dei movimenti con indicazione delle operazioni disconosciute (data e luogo) effettuate con bancomat/carta di credito (se possibile estratto conto degli ultimi mesi);
- indicazione degli ultimi luoghi in cui è stata utilizzata la carta (prelievi ATM, esercizi commerciali, siti internet, etc.);
- destinazione data alla somma sottratta (versamento su conto corrente, su carta ricaricabile, ricarica di sim card di telefonia mobile, pagamenti online, etc.).

Sarà utile acquisire nel corpo della denuncia il totale delle somme disconosciute, annotando le varie operazioni utilizzando il seguente schema:

Data e ora dell'operazione	Descrizione	Addebiti
L'ora non sempre è disponibile	*Luogo reale (acquisto in negozio o ritiro presso ATM) o virtuale dove avvengono le spendite*	*Importo addebitato*

Accertamenti minimi richiesti

Nel caso sub A), le spendite saranno effettuate *on line* su vari siti di *e-commerce* o per effettuare ricariche di vario genere (conti gioco on line e sim telefoniche nella maggioranza dei casi).

1) Spendite su siti *e-commerce* - Si rappresenta che, nell'ipotesi in cui le spendite vengano effettuate sui siti internet allocati all'estero, seppur siano possibili accertamenti con la collaborazione dell'Interpol o con l'inoltro di richieste di assistenza giudiziaria internazionale, tali richieste non vengono quasi mai inoltrate poiché, esperienze maturate sul campo, hanno evidenziato la problematica inerente alla tempistica elevata per ottenere una risposta, tale da far perdere completamente le tracce del reo. È trasmettere la *notitia criminis* con l'indicazione che le spendite sono state effettuate all'estero (*indicare in quale stato estero risulta avere sede il sito e-commerce*) e che non vi sono ulteriori elementi per il prosieguo dell'attività di indagine sul territorio nazionale.

Per quanto attiene alle spendite sui siti e-commerce italiani (negozi di materiale informatico, acquisti di biglietti aerei o ferroviari, ecc.) basterà richiedere le informazioni dettagliate all'ufficio legale del sito[25], richiedendo:

- indirizzo IP e dati inseriti nel form di registrazione (da cui sarà ricavabile un nominativo e verosimilmente l'utenza di contatto),
- indirizzo IP relativo all'acquisto fornendo il numero e la data di scadenza della carta di credito, nonché il dettaglio del movimento disconosciuto dal denunciante,
- l'indirizzo, il numero di spedizione e il corriere utilizzato,
- copia dell'estratto conto sul quale sia confluito il profitto delle operazioni.

2) Ricariche conti gioco su siti di gioco e scommesse on line - Nel caso in cui la movimentazione disconosciuta venga dirottata verso siti di giochi *on line*, le informazioni dettagliate dovranno essere richieste all'ufficio legale delle società (normalmente all'interno di ogni sito è indicato un punto di contatto), fornendo il numero e data di

[25] Normalmente all'interno di ogni sito è indicato un punto di contatto.

scadenza della carta di credito, i dettagli della transazione (data ora e numero della transazione), richiedendo:

- il numero del conto gioco ricaricato,
- indirizzo IP e dati inseriti nel *form* di registrazione del titolare del conto gioco,
- eventuali documenti di identificazione allegati alla registrazione,
- indirizzo IP relativo alla transazione di ricarica del conto gioco,
- modalità di gioco da parte del titolare del conto (tavoli *cash*, rosso e nero etc.),
- dati dettagliati di eventuali giocatori "*collusi*" con il titolare del conto gioco di partenza (esempio: consecutive perdite a favore di un altro giocatore).

3) Ricariche telefoniche - In questo caso le informazioni dettagliate dovranno essere richieste all'ufficio legale dei vari gestori telefonici interessati, fornendo il numero e data di scadenza della carta di credito, i dettagli della transazione (data ora e numero della transazione), richiedendo:

- l'utenza ricaricata,
- il nominativo dell'intestatario dell'utenza,
- l'eventuale ricezione sull'utenza individuata di ulteriori ricariche effettuate mediante l'utilizzo di altre carte di pagamento e/o credito.

Nel caso sub B), le transazioni disconosciute saranno effettuate mediante prelievi su ATM o spendite su negozi tradizionali sparsi sul territorio nazionale. La prima attività da effettuare è l'acquisizione delle immagini del sistema di videoregistrazione dal servizio di sicurezza sia dell'Istituto bancario dove è stato applicato il sistema di intercettazione dati (*skimmer*), sia presso lo sportello dove il denaro viene prelevato (immediatamente rintracciabili nella denuncia, in quanto risulta essere l'Atm dove viene effettuato l'ultimo prelievo riconosciuto e l'Atm dove vengono effettuati i successivi prelievi disconosciuti). In questo caso, è possibile rinvenire indicazioni valide solo per un breve periodo dall'evento (di solito non oltre i 7 giorni), laddove il sistema di videoregistrazione sia funzionante e opportunamente posizionato.

Può essere importante risalire con immediatezza al punto di compromissione (ovvero l'ultimo luogo ove è stata spesa la carta in maniera genuina) per capire se le carte vengono acquisite con sistemi fraudolenti da personale interno: tuttavia, di regola l'analisi delle spendite fraudolente finalizzata alla ricerca di punti di compromissione viene effettuata direttamente dai gestori delle carte di credito, che predispongono autonomamente specifiche e complessive denunce/querele alla luce di quanto emerso da tali analisi.

In ogni caso, gli accertamenti sull'esatta ubicazione degli esercizi commerciali presso cui è stata utilizzata fraudolentemente la carta di credito, e/o degli sportelli ATM presso i quali sono stati effettuati i prelievi, e sull'eventuale acquisizione delle immagini registrate in virtù di telecamere funzionanti direzionate nella zona dell'ATM possono essere effettuati direttamente dall'ufficio competente per territorio che ha ratificato la denuncia, non essendo necessarie precise competenze specialistiche

Pregresse esperienze investigative

Nel caso sub A) nr. 1, esperienze investigative pregresse hanno evidenziato che sia le utenze telefoniche associate agli indirizzi IP che i dati di registrazione, nella maggior parte dei casi, corrispondono a nominativi fittizi o collegabili a persone che hanno subito un

furto di identità o un'intrusione telematica. Per quanto attiene alle utenze, queste sono o di fantasia o fittiziamente intestate (in questo caso sarà utile contattare il corriere per acquisire eventuali ulteriori utenze che siano collegate al ricevimento del pacco in questione). Di conseguenza, la strategia investigativa più utile sarà quella di monitorare la consegna della merce (che normalmente avviene entro 4-5 giorni dall'acquisto) al fine di individuare il luogo esatto del ritiro e la persona che effettivamente provvede a ritirare la merce.

Nel caso sub A) nr. 2, esperienze investigative maturate hanno evidenziato che il *modus operandi* relativo alle ricariche dei conti gioco risulta essere il seguente: l'importo di denaro viene versato su un conto gioco "*non verificato*" (si intende privo della certa identificazione del titolare che non ha ancora trasmesso la copia del proprio documento a supporto della propria registrazione). Il titolare di un conto "*non verificato*" può ricaricare il conto, giocare (vincere e/o perdere), ma non può monetizzare ovvero richiedere l'incasso delle somme presenti sul conto gioco. Tale situazione fa sì che le somme confluite sul predetto conto gioco vengano, normalmente, perse, con uno o più passaggi a favore di altri giocatori "*verificati*", i quali possono ritirare o perdere a favore di altri giocatori (il più delle volte su altre piattaforme di gioco per ritardare l'attività investigativa). A tal proposito, giova rappresentare che nella maggioranza dei casi o il giocatore "*verificato*" ha fornito un documento falso o contraffatto ovvero il giocatore "*verificato*" è una persona che ha ceduto la propria identità in cambio di denaro (esempio: tossicodipendenti, stranieri senza fissa dimora o indigenti).

Nel caso sub A) nr. 3, normalmente gli intestatari sono nominativi fittizi o persone compiacenti difficilmente rintracciabili (esempio, stranieri senza permesso di soggiorno o senza fissa dimora).

Nel caso sub B), gli accertamenti sulle spendite effettuate in Italia presso esercizi commerciali a distanza di tempo rispetto ai fatti non permettono l'ottenimento di indicazioni utili, a causa delle scarse indicazioni che l'addetto al pagamento può fornire, tranne nei casi di spese rilevanti in negozi con limitato flusso di clienti (per esempio, gioiellerie o concessionari di grandi marche).

Solamente laddove gli indagati siano trovati nel materiale possesso di carte di credito sarà possibile applicare l'art. 493 ter c.p., anche al fine dell'arresto nella flagranza del reato. Spesso invece la Polizia Giudiziaria - intervenuta sul posto - procede a contestare tale norma anche laddove sia stato ritrovato, di regola apposto su uno sportello ATM (cd sportello bancomat), apparecchiature (cd *skimmer*) idonee alla captazione dei codici presenti nella banda magnetica delle carte. In questi casi, invero, la norma più aderente ai fatti è quella ex art. **617-quinquies** c.p. *(installazione di apparecchiature atte ad intercettare la comunicazione intercorrente tra il chip della carta di credito e il sistema informatico dell'istituto di credito)* che consente ugualmente l'arresto (facoltativo) in flagranza. Difficile, infatti, sostenere come in tale ipotesi possa venire in rilievo qualcuna della condotte previste dall'art. 493 ter c.p., sia pure nella forma del tentativo.

È consigliabile comunque, anche in questi casi, procedere subito all'analisi tecnica (da ritenersi pacificamente di carattere ripetibile) dello *skimmer* sequestrato, dal momento che il ritrovamento di numerazioni di carte di credito all'interno di esso potrà a questo punto configurare anche l'ipotesi della detenzione di carte di credito o, secondo altra

impostazione teoricamente sostenibile, quella di cui all'art. **615-quater** c.p. (dal momento che, con tale condotta - di regola accompagnata anche dalla acquisizione, tramite meccanismi di videoripresa, dei relativi codici PIN all'atto della loro digitazione - , abusivamente l'agente si procura codici di accesso al sistema informatico della banca).
Ove, invece, si sia proceduto all'arresto in relazione all'accertato possesso di carte di credito contraffatte, la Polizia Giudiziaria dovrà porre in essere tutti gli accertamenti necessari su quanto in sequestro al fine di verificare la illecita provenienza dei supporti magnetici.

Diffamazione online

Qualificazione giuridica

Art. 595 c.p. – Diffamazione (competenza non distrettuale)

Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a euro 1.032..... Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a euro 516.

Fenomeno

La persona offesa denuncia la presenza sulla rete internet (sito internet, blog, forum online, profilo/gruppo/ pagina social) di una pubblicazione lesiva del proprio onore/reputazione.

Elementi da acquisire in denuncia

Giorno in cui si è avuta cognizione della pubblicazione; indicazione di tutti i luoghi virtuali dove è presente la pubblicazione lesiva, evidenziando l'URL della pagina, ovvero il nome delle comunità virtuali, Id o *nick name* dell'autore della pubblicazione illecita; copia del contenuto illecito (copia della pagina *web*, del video, dell'immagine, del messaggio o dell' e-mail comprensiva di *header*); indicazione dei nominativi e dei recapiti delle persone che hanno visualizzato la pubblicazione; indicazione di eventuali situazioni personali e/o professionali che potrebbero essere alla base del commento diffamatorio; eventuale istanza al fornitore del servizio di rimozione dei contenuti offensivi (che, qualora effettuata, rende impossibile la valutazione degli stessi).

Accertamenti minimi richiesti

La Polizia Giudiziaria provvederà a verificare se la pagina (o il messaggio sul forum o del blog) è ancora presente, dandone riscontro nella CNR, e a informare il denunciante che la richiesta di rimozione della pagina o del *post* diffamatorio può essere avanzata direttamente dal medesimo al gestore della piattaforma. È importante ribadire che se la persona offesa non è in grado di produrre la copia della pagina web o l'URL, nessun tipo di accertamento sarà possibile.
Una volta acquisito il commento/post diffamatorio e il nome del sito/social network su cui è stato pubblicato, fornendo all'ufficio legale di contatto il nome dell'utente autore dello stesso, bisognerà: acquisire il *form* di registrazione dell'utente con i dati, comprensivo di indirizzo email, nonché l'indirizzo IP di connessione; acquisire l'indirizzo IP di

inserimento del commento/*post* diffamatorio.

Pregresse esperienze investigative

Si registra un aumento esponenziale di fascicoli che riguardano i reati di diffamazione (*ma anche stalking, cyberbullismo e molestie*) che avvengono mediante *social network*, siti internet o blog avente sedi legali all'estero.

Per quanto attiene i più famosi *social network* si potrà richiedere tramite decreto dell'A.G. competente l'acquisizione dei log di connessione a un determinato *account,* nonché i dati di registrazione e la casella di posta elettronica utilizzata in fase di registrazione dell'*account* stesso come di seguito indicato.

Il canale più veloce di contatto con Facebook sarà tramite il portale raggiungibile all'URL: *https://facebook.com/records*, all'interno del quale mediante una procedura molto semplice potranno essere richiesti i dati necessari alla prosecuzione dell'indagine di un determinato *account facebook* che sarà individuato da un identificativo (*Profil-ID*). Si rappresenta che lo stesso portale può essere utilizzato per gli *account* delle società *Instagram* e *Whatsapp*.

Per quanto riguarda il *social network Twitter*, si potrà contattare la società tramite il portale raggiungibile all'indirizzo: *https://support.twitter.com/forms/lawenforcement*.

Si rappresenta che il reato di **diffamazione**, così come individuato dalla normativa italiana, non consente l'acquisizione dei predetti dati se non a seguito di richiesta di assistenza giudiziaria internazionale (rogatoria), in quanto tale reato non è contemplato nella legislazione statunitense (sede dei maggiori *social network*, siti o blog presenti in rete).

Furto di telefono o altra apparecchiatura informatica

Qualificazione giuridica

artt. 624 c.p. – Furto (competenza non distrettuale)

Chiunque s'impossessa della cosa mobile altrui, sottraendola a chi la detiene, al fine di trarne profitto per sé o per altri, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 154 a euro 516.

Fenomeno

Il furto di tali sistemi informatici è sempre più diffuso, ma l'attività di indagine non comporta alcuna conoscenza tecnica o utilizzo di apparecchiatura informatica.

Elementi da acquisire in denuncia

Giorno e luogo dell'evento e quant'altro si ritenga utile; marca, modello e qualora possibile numero seriale dell'apparecchio; numero IMEI dell'apparecchio telefonico o informatico (esempio *tablet* con accesso a *internet* tramite scheda dati, anch'esso avrà un numero IMEI); numero telefonico della SIM associata all'apparecchio; società di gestione del contratto telefonico e/o telematico della SIM (Telecom, Vodafone, Wind, etc.); indicare se il denunciante ha già bloccato la SIM derubata e l'abbia sostituita.

Accertamenti minimi richiesti

La Polizia Giudiziaria provvederà a richiedere fin da subito un decreto per acquisire il tabulato di traffico telefonico e/o dati dell'IMEI dell'apparecchio dal giorno del furto compreso, alla data di emissione del predetto provvedimento. All'esito, basterà verificare l'ultimo utilizzatore dell'apparecchio per recuperare l'oggetto rubato, procedendo alla riconsegna, salvo contrario avviso dell'A.G., mediante verbale all'avente diritto.
Si rappresenta che la Polizia Postale e delle Comunicazioni non è in possesso di nessuna apparecchiatura speciale per rinvenire tale tipologia di oggetti.

Pregresse esperienze investigative
Si evidenzia che nella maggioranza dei casi, l'ultimo utilizzatore non è completamente a conoscenza della provenienza illegale dell'oggetto, quindi basterà convocarlo e richiedere la riconsegna dello stesso (che quasi sicuramente avrà portato con sé), redigendo nei suoi confronti un verbale di elezione di domicilio e nomina difensore quale persona indagata per il reato di ricettazione di cui all'art. 648 c.p., ovvero di incauto acquisto ex art. 712 c.p..

Altro reato informatico come da SICIP

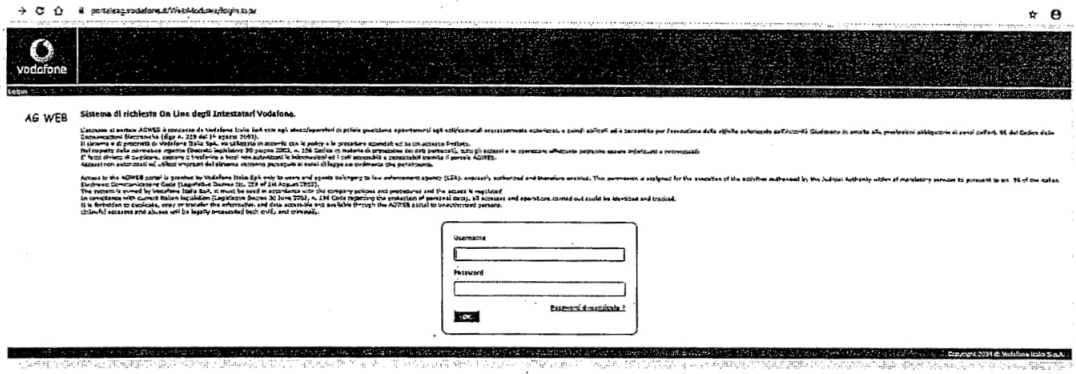
Ove un fatto di reato non rientri nelle categorie precedentemente illustrate, e sempre che non si tratti di reato attinente la ***pedopornografia online, la protezione infrastrutture critiche, la criminalità informatica altamente specializzata*** **(per cui la Polizia delle Comunicazioni ha una competenza esclusiva** - vedasi art. 51 comma 3 quinquies C.P.P. e D.M. del 15/08/2017), occorrerà individuare la corretta qualificazione giuridica tra le seguenti qui riportate:
art. 617-*bis* c.p. (installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche);
art. 617-*ter* c.p. (falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche);
art. 617-*quater* c.p. (intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche);
art. 617-*quinquies* c.p. (installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche);
art. 617-*sexies* c.p. (falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche);
art. 635-*bis* c.p. (danneggiamento di informazioni, dati e programmi informatici);
art. 635-*ter* c.p. (danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da un altro ente pubblico o comunque di pubblica utilità);
art. 635-*quater* c.p. (danneggiamento di sistemi informatici e telematici);
art. 635-*quinquies* c.p. (danneggiamento di sistemi informatici e telematici di pubblica utilità);
art. 640-*quinquies* c.p. (frode informatica del soggetto che presta servizi di certificazione di firma elettronica).

Di seguito Troviamo invece i portali delle forze dell'ordine e i numeri di riferimento per le stesse

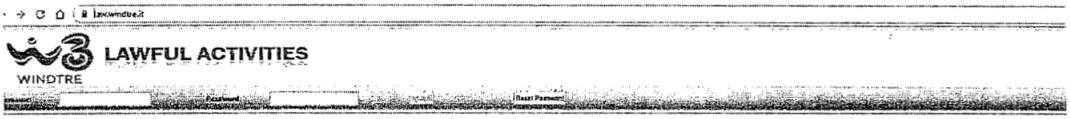
Approfondimento tecnico

I gestori mettono a disposizione della polizia giudiziaria dei portali attraverso i quali è possibile richiedere i dati telematici di accesso.

Vodafone: https://portaleag.vodafone.it



Wind: https://law.windtre.it/

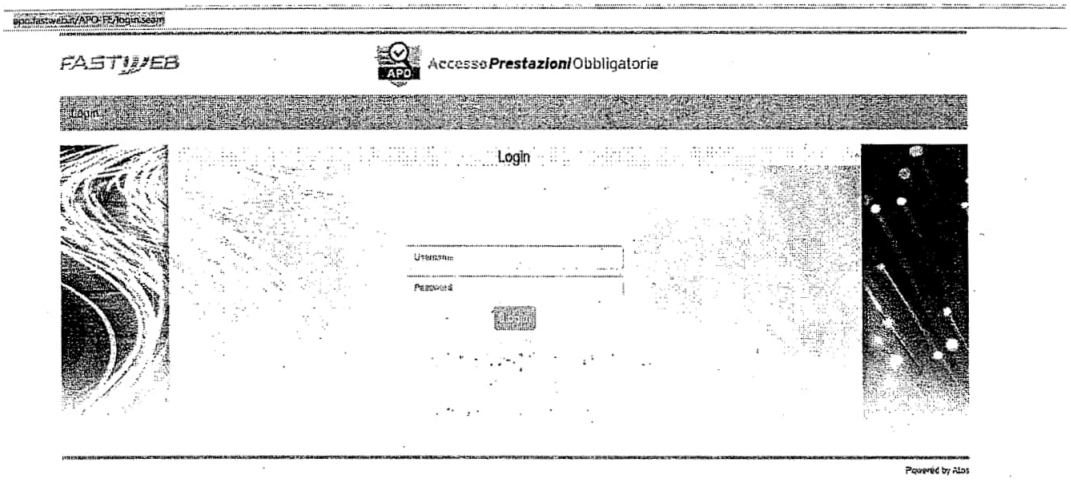


— AVVISO —
Vi informiamo che,

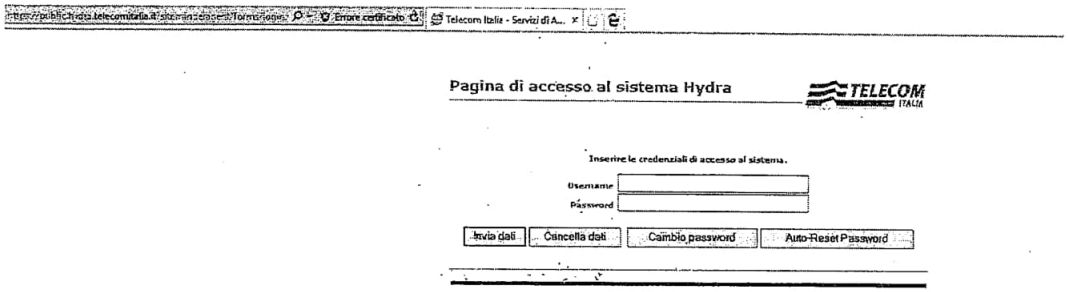
- con Provvedimento nr. 356 del 18 luglio 2013 del Garante per la Protezione dei Dati Personali, successive proroghe e in ultimo quella del 26 gennaio 2017 con il quale veniva sospesa l'entrata in vigore delle Prescrizioni impartite sino al 31 dicembre 2017, si rende noto che essendo ormai abbondantemente scaduta tale proroga, dovendo questa society comunque adottare una serie di ulteriori misure di sicurezza fisica ed informatica e provvedere alla dismissione dei suddetti canali di trasmissione a ricezione analogica entro e non oltre il 12 ottobre 2020, si richiede che non vengano piu' inviati a questo Operatore Telefonico richieste anagrafiche, di traffico storico e di intercettazioni per il tramite di fax analogici e, nel contempo, di utilizzare esclusivamente le apposite funzionalita' presenti ed attive sul Portale LAW.
- L'azienda sta cominciando l'avvio dell'estensione a tutta l'utenza Wind Tre S.p.A. del servizio VoLTE, pertanto la nostra societa' e' nelle condizioni di assicurare e garantire le Prestazioni Obbligatorie previste dall'art. 96 del C.C.E..
- in esecuzione di un piu' ampio accordo commerciale, a far data dal 5 marzo 2020 e' iniziata la migrazione, verso la Rete mobile di Wind Tre, delle utenze del Mobile Virtual Network Operator (MVNO) e Mobile Network Operator (MNO) Fastweb, provenienti dal precedente Operatore ospitante.
- In data 24 febbraio 2020 e' iniziata la commercializzazione di un nuovo Prodotto e Servizio di telefonia denominato 'Very Mobile', le Prestazioni Obbligatorie previste dall'art. 96 del Codice delle Comunicazioni, non trattandosi di un nuovo o diverso Operatore ma di un mero Servizio, saranno garantite integralmente ed assicurate all'Autorita' ed alla Polizia Giudiziaria da questo Operatore Telefonico.
- Ricordiamo che a far data dal 6 Marzo 2019, a seguito della stipula di apposita Convenzione tra il Ministero dell'Interno e la Wind Tre S.p.A. che, giusto art. 55, comma 7, del Codice delle Comunicazioni Elettroniche, ha permesso di regolamentare l'accesso telematico delle Forze di Polizia e dell'Autorita' Giudiziaria ai dati degli utenti di telefonia fissa e mobile, sara' attivo un collegamento informatico che consentira', autonomamente e per il tramite del Centro di Elaborazione Dati (CED) del Dipartimento della Pubblica Sicurezza, di consultare l'Elenco Telefonico Nazionale (ETNs). In adempimento alle prescrizioni del Garante per la Tutela dei Dati Personali, con l'entrata in funzione di ETNs e' prevista la disabilitazione delle funzionalita' di richiesta anagrafica agli Operatori appartenenti alle Forze di Polizia di cui all'Art. 16 della legge 121/81. Tuttavia, al fine di garantire la continuita' del servizio sia alle Forze di Polizia delegate dall'Autorita' Giudiziaria che alla Polizia Giudiziaria agli Operatori non appartenenti alle Forze di Polizia di cui all'Art. 16 della legge 121/81, operante d'iniziativa nell'ambito dei poteri e delle facolta' riconosciutegli dall'art. 55 del c.p.p., la nostra society implementera' sui consueti canali (Portale LAW) un'apposita dichiarazione di responsabilita'. Solo successivamente all'accettazione di tale informativa e dichiarazione, difatti, sara' possibile proseguire.
- SI RICORDA CHE LE ATTIVITA' DI INTERCETTAZIONE VENGONO, COME DI CONSUETO, EVASE NEI GIORNI FERIALI ED IN ORARIO DI LAVORO (08.30/17.30). EVENTUALI RICHIESTE NOTIFICATE FUORI DAI SUDDETTI ORARI FERIALI (IN PARTICOLARE NEI GIORNI DI SABATO, DOMENICA, FESTIVI E DALLE 17.31 SINO ALLE 08.29) POTRANNO ESSERE CORRETTAMENTE ASSICURATE SOLO CONTATTANDO IL SERVIZIO DI REPERIBILITA' ALLE NUMERAZIONI DEDICATE.

Inoltre al fine di garantire la coerenza dei dati estratti con quanto da Voi richiesto, vi saremmo grati se, prima di iniziare la sessione di consultazione, voleste procedere alla c.d. 'pulizia della cache' cosi' da evitare possibili incongruenze tra la Vostra sessione di lavoro e quanto precedentemente memorizzato dai browsers di navigazione presenti sul Vostro computer.

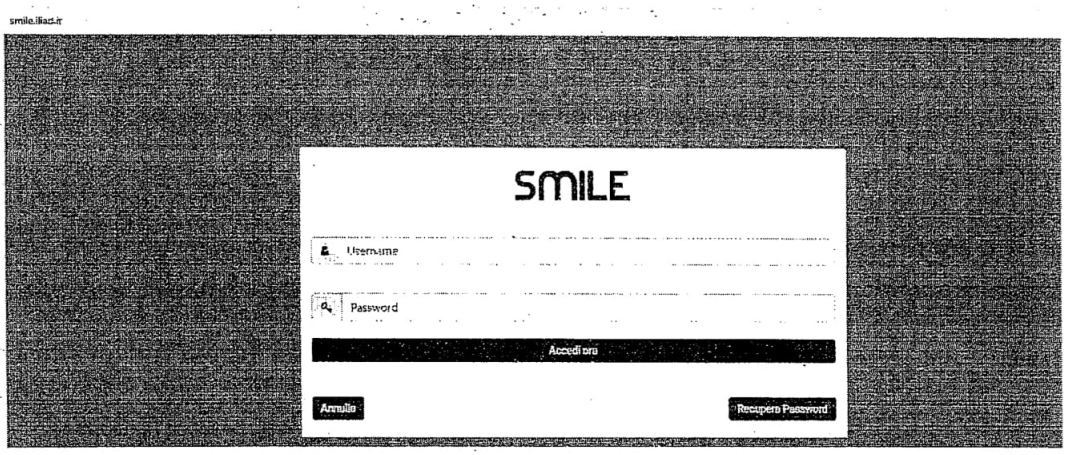
Fastweb: https://apo.fastweb.it/APO-FE/login.seam



Telecom: https://public.hydra.telecomitalia.it

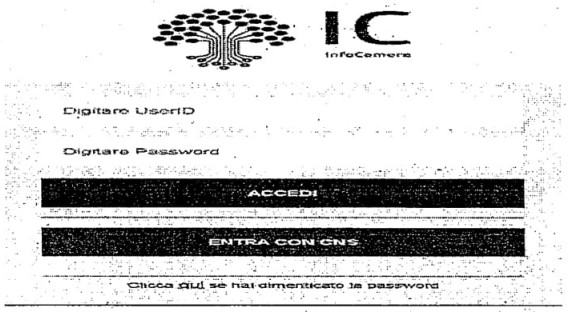


Iliad: https://smile.iliad.it/

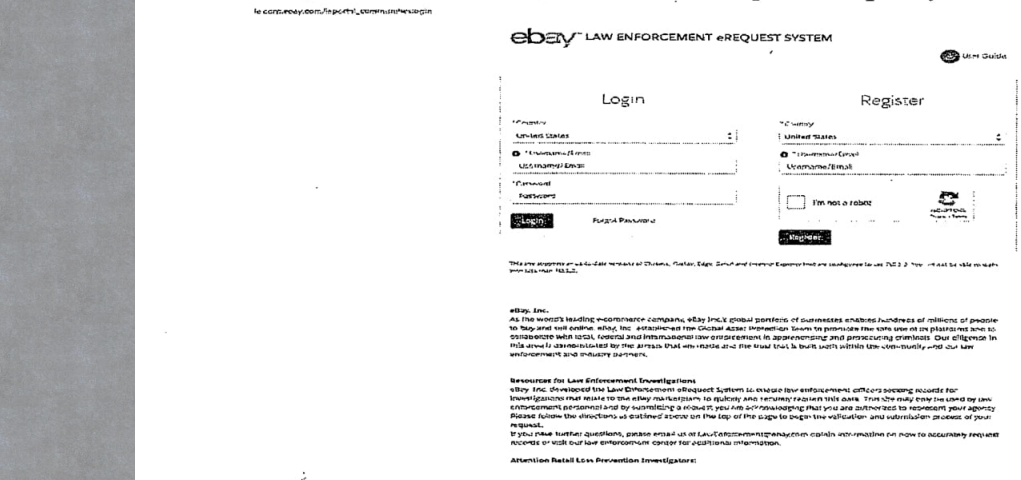


Poste Italiane: https://posteag.poste.it

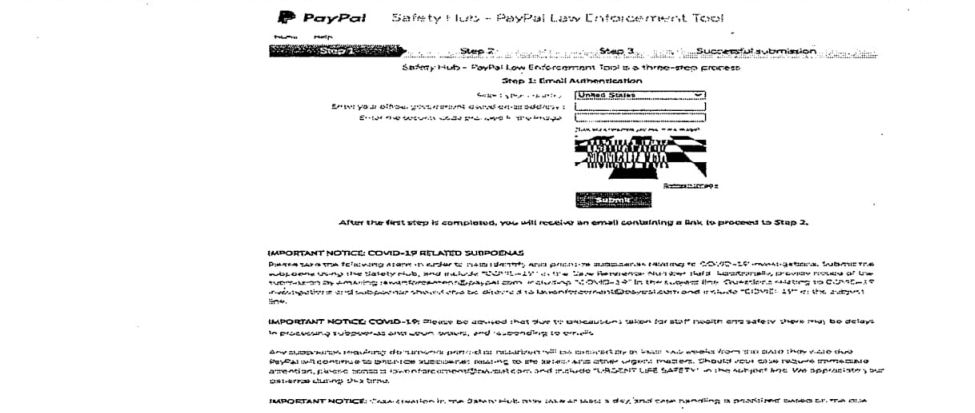
Camera di Commercio: https://login.infocamere.it/eacologin/login.action



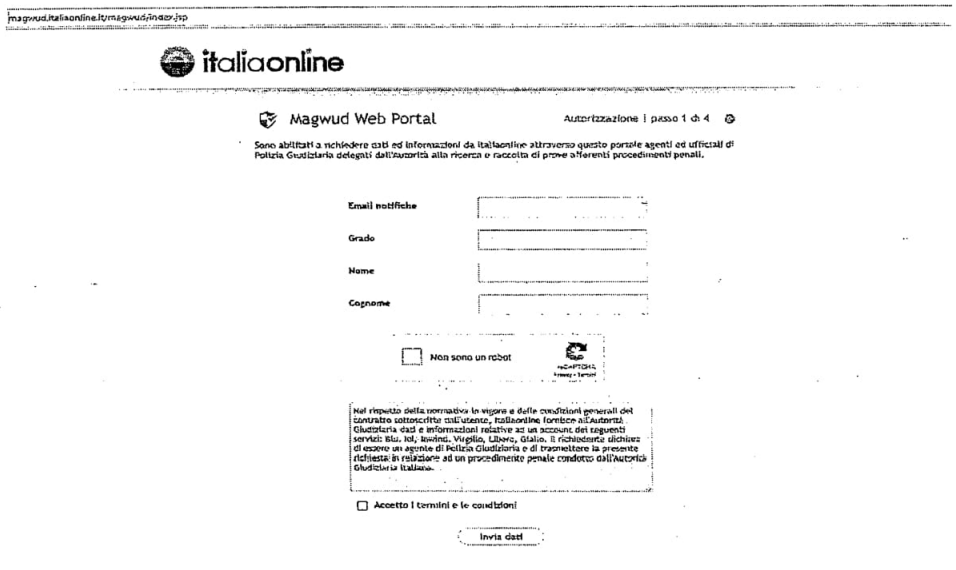
Ebay: dominio ufficiale portale FF.OO: https://le.corp.ebay.com



Paypal: https://safetyhub.paypalcorp.com/AIP/portal/home.do



ItaliaOnLine (Libero.it, Virgilio.it, Iol.it): https://magwud.italiaonline.it/

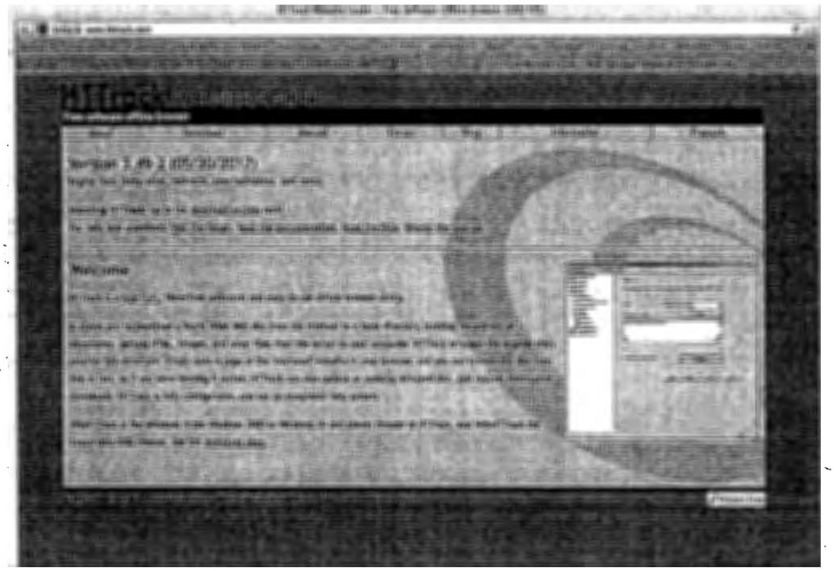


[redacted]

Approfondimenti tecnici di base

Acquisire sito/pagina web

Per acquisire una pagina e/o un sito web si può utilizzare HTTrack Website Copier, programma gratuito e open source, disponibile per sistemi operativi Windows, Linux e Mac OS X. HTTrack Website Copier è scaricabile all'url http://yvww.httrack.com , dove c'è una guida per l'utilizzo.
E' possibile scaricare interi siti web creando una copia locale completa di codice HTML, scripts, immagini ed altri files, e può aggiornare copie locali già esistenti aggiungendo i nuovi contenuti; al termine viene creato un log dell'attività.
Quanto ottenuto dall'acquisizione può essere visualizzato con il browser preferito.
Il programma può essere installato oppure può essere utilizzato standalone (ad esempio su una chiave USB senza bisogno di installazione).
Il programma permette la personalizzazione della configurazione dell'acquisizione: livello di profondità, limiti di banda, numero di connessioni contemporanee, filtri per esclusione contenuti e/o links ed altri parametri.



Più empiricamente è possibile acquisire la sola pagina web utilizzando l'opzione di salvataggio dei browser di navigazione.

Leggere e stampare header delle email

Il messaggio di posta elettronica o e-mail è costituito da: 1)una busta - envelope (per busta si intendono le informazioni a corredo del messaggio che vengono scambiate tra server attraverso il protocollo SMTP); 2) un corpo del messaggio – body (testo e allegati che costituiscono il contenuto informativo del messaggio; 3) una sezione di intestazioni (header).

Le intestazioni (header), o proprietà di una mail, sono informazioni di servizio che servono a controllare l'invio dei messaggio, o a tener traccia delle manipolazioni che subisce. Ciascuna intestazione è costituita da una riga di testo, con un nome seguite dai carattere e dal corrispondente valore. Alcune di queste vengono definite e possono essere modificate direttamente dall'utente. Tra le principali si possono citare:

Subject: (Oggetto:) dovrebbe contenere una breve descrizione dell'oggetto del messaggio;
From: (Da:) contiene l'indirizzo di posta elettronica del mittente;
To: (A:) contiene gli indirizzi di posta elettronica dei destinatari principali;
Cc: contiene gli indirizzi di posta elettronica dei destinatari in copia conoscenza (Carbon Copy);
Reply-to: (Rispondi a:) contiene l'indirizzo di posta elettronica al quale devono essere inviate le eventuali risposte al messaggio, se diverso da quello del mittente;
Date: (Data:) contiene la data e l'ora in cui il messaggio è stato scritto.

Le intestazioni di servizio vengono aggiunte dai programmi che manipolano il messaggio. La più importante è *Received:*, che viene aggiunta da ciascun server SMTP che manipola il messaggio, indicando da quale indirizzo IP il messaggio è stato ricevuto, a che ora, e altre informazioni utili a tracciarne il percorso. Giova sottolineare che le email gestite dal Web adoperano l'IP del gestore (server di Posta).

Il *Message-ID:* *(Identificativo del messaggio)* è un codice costruito dal client su cui il messaggio è stato composto, che dovrebbe permettere di identificare univocamente un messaggio del MTA (Mail Transfer Agent) incaricato dell'inoltro.

La visualizzazione delle intestazioni (header), varia a seconda dei client e/o delle webmail di posta utilizzate.

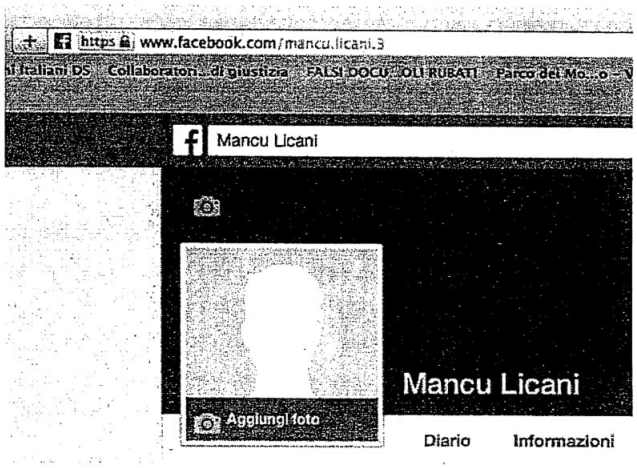
Si precisa che tramite le app di Android e Ios non è possibile visualizzare l'header di una mail.

Esempio:

SOCIAL NETWORK

Facebook – Accertamenti di Polizia Giudiziaria: ID Utente

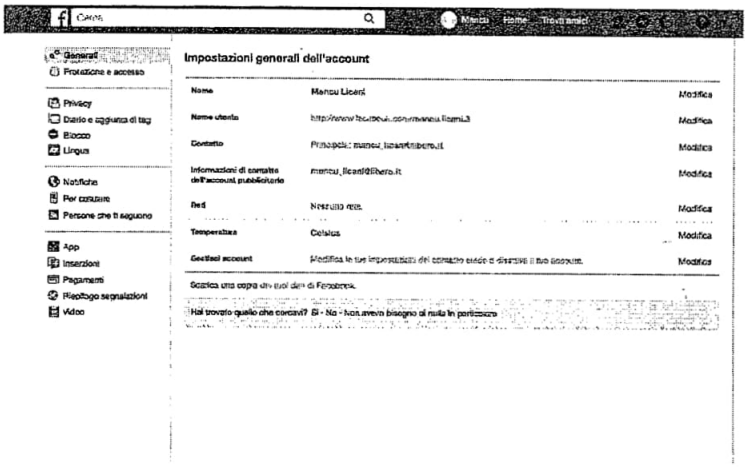
Ogni utente ha un identificativo univoco, ricavabile dalla URL del profilo:

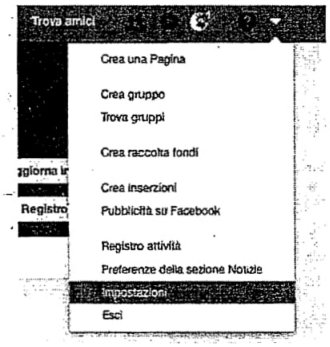


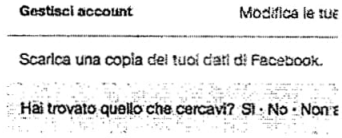
Alla società che gestisce Facebook, nel caso necessiti l'identificazione dell'utilizzatore di un profilo, va richiesta tale informazione inserendo nella richiesta non il nome che compare nella pagina del profilo bensì l'account che compare nell'url, unico dato univoco che identifica l'utente. Senza tale informazione non è possibile effettuare richieste di alcun genere.

Analogo discorso per Pagine e Gruppi

Nel momento in cui si ha la disponibilità dell'accesso all'account è possibile effettuare il download completo di tutte le attività svolte attraverso l'account stesso







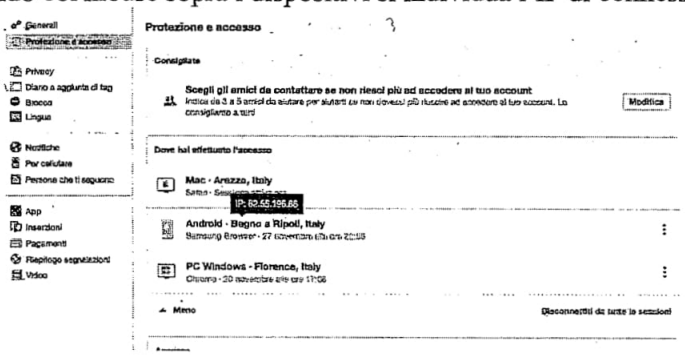
La copia dei dati di un account non è sempre contemporanea alla richiesta e questo a causa della mole dei dati da acquisire. Tale copia viene inviata all'account di posta elettronica inserito al momento della registrazione dell'account stesso.

Altri social network

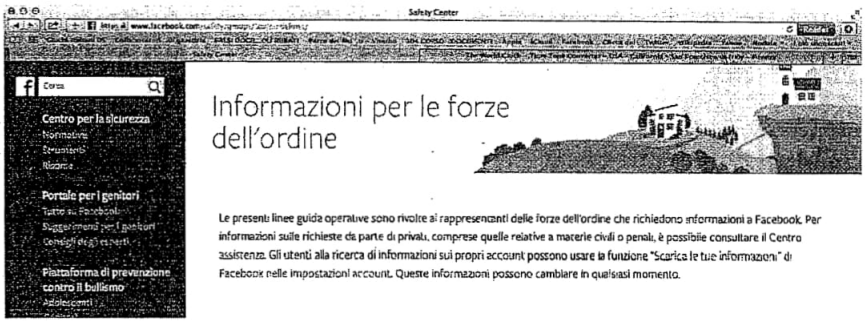
Come per Facebook anche social network come Twitter, Instagram ed altri funzionano con la medesima modalità, è necessario identificare l'account univoco dell'utente piuttosto che il nome che viene visualizzato.

Ultimi accessi e dispositivi

Da "impostazioni" cliccare su "Protezione e Accesso" e nella sezione "Dove hai effettuato l'accesso" passando col mouse sopra i dispositivi si individua l'IP di connessione



Linee Guida per le Forze dell'Ordine



Richieste di emergenza

Qualora siano necessari il rilascio immediato di informazioni e l'intervento in caso di pericolo imminente per un bambino o rischio di morte o serio danno fisico a una persona, un rappresentante delle forze dell'ordine può inviare una richiesta usando il sistema per le richieste online delle forze dell'ordine.

Nota: Facebook non legge né risponde alle richieste inviate da persone che non sono rappresentanti ufficiali delle forze dell'ordine. Gli utenti a conoscenza di una situazione di emergenza devono contattare immediatamente e direttamente le forze dell'ordine locali.

Requisiti delle richieste

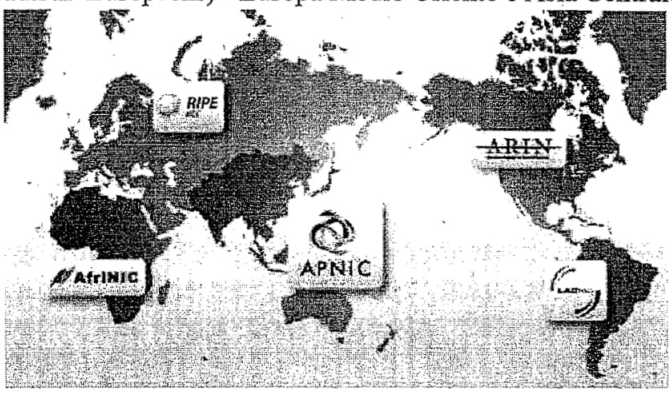
Non verranno elaboratele richieste troppo vaste o vaghe. Tutte le richieste devono indicare: 1) Il nome dell'autorità richiedente, 2) il numero dell'ID dell'agente responsabile, 3) l'indirizzo e-mail con un dominio delle forze dell'ordine e un numero di telefono diretto, 4) l'indirizzo e-mail, 5) il numero dell'ID utente (http://www.facebook.com/profile.php?id=1000000XXXXXXXX) o il nome utente (http://www.facebook.com/username) del profilo Facebook

Siti internet di e-commerce

I siti internet di e-commerce usano come identificazione sempre un Id univoco, dell'utente o dell'annuncio di vendita che va ricercato nell'url dell'annuncio o viene indicato nell'annuncio stesso.

Verificare l'allocazione di una pagina su Internet e le informazioni di registrazione

Anche se non attendibili al 100%, esistono dei modi semplici per la Polizia Giudiziaria per verificare - da una postazione Internet - su quali server (italiani o esteri) una pagina web è allocata.
Gli indirizzi IP pubblici sono rilasciati e regolamentati dall'ICANN tramite i seguenti organi preposti all'assegnazione degli indirizzi IP nel mondo:
AfriNIC (African Network Information Centre) - Africa
APNIC (Asia Pacific Network Information Centre) - Asia e Oceano Pacifico;
ARIN (American Registry for Internet Numbers) – Nord America
LACNIC (Regional Latin-American and Caribbean IP Address Registry - America Latina e Caraibi)
RIPE NCC (Rèseaux IP Europèens) - Europa Medio Oriente e Asia Centrale



I siti internet attraverso cui poter effettuare gli accertamenti in merito all'assegnazione degli indirizzi IP sono molteplici, di seguito se ne indicano alcuni:

https://whois.domaintools.com

https://www.ipinfo.io

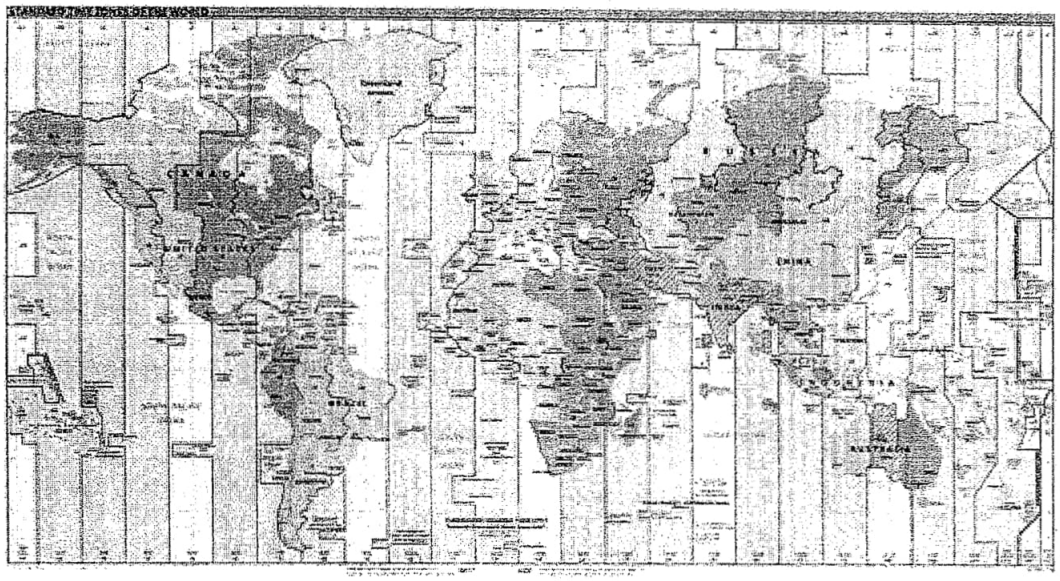
https://www.infobyip.com

http://www.centralops.net

Tali siti internet, interrogando gli organi sopra menzionati, forniscono le informazioni necessarie per l'identificazione del gestore a cui, localmente, è assegnato a sua volta l'indirizzo IP di interesse.

Il fuso orario

I dati forniti dai gestori indicano sempre il fuso orario di riferimento e questo perché i server che registrano le informazioni di registrazione o i dati di accesso di un utente sono configurati in base ad un fuso orario che, se il gestore è italiano, non necessariamente è impostato allo stesso modo, ma generalmente è configurato come GMT cioè il fuso orario di Londra, riconosciuto come punto di riferimento internazionale.
Allo stesso modo gestori stranieri utilizzeranno il fuso orario del loro paese o un fuso orario che per loro è di riferimento.

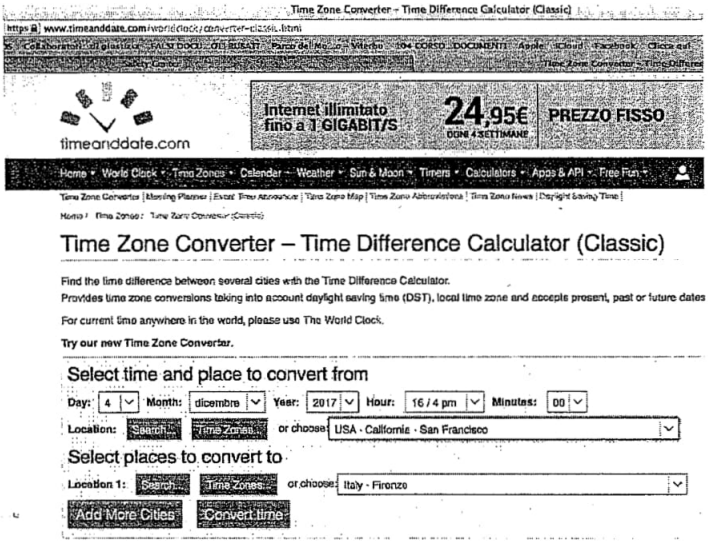


Per questo motivo nelle richieste di emissione di decreti di acquisizione file di log viene menzionato il fuso orario di riferimento o vengono convertiti i dati forniti nel fuso orario del gestore per evitare di creare confusione nelle richieste.

Un sito internet molto utile per la conversione di date e orari nel fuso orario del paese di riferimento è TimeZoneConverter raggiungibile all'indirizzo

http://www.timeanddate.com

che permette di inserire una data ed un orario con il suo fuso orario di riferimento allo scopo di convertirlo nel fuso orario di interesse.



RIFERIMENTI UTILI PER LA POLIZÌA GIUDIZIARIA

I) TRUFFE *ONLINE* (eBay o altre piattaforme di commercio elettronico o bacheche di annunci)

■ Il settore *Fraud Investigation Team* di Ebay è contattabile ai seguenti recapiti:

eBay Europe S.a.r.l. 22-24 Boulevard Royal, L-2449 Lussemburgo, e-mail: forzedellordine@ebay.com, fax 0230-410366.

■ Altre piattaforme di commercio elettronico o bacheche annunci:

- **ANNUNCI.NET** – 333/2692920-----FAX 02/70039532;
- **BAKECA.IT** – 011/6395003-----FAX 011/6503031;
- **BACHECAANNUNCI.IT** – 01/8557880-----FAX 010/91631154;
- **SECONDAMANO.IT** – TEL. 02/56789-----FAX 02/56787700;
- **SUBITO.IT** – TEL. 0236637008-----FAX 02/93664563.
- **KIJIJI** ha sede a Marktplaats B.V Wibautstraat 224 1097 DN Amsterdam The Netherland. E' contattabile ai seguenti recapiti:
  E-mail: forzedellordine@ebay.com ----- FAX 02/30410366.

II) CARTE DI CREDITO PREPAGATE (ricaricabili)

■ Per gli accertamenti sulle carte prepagate di **Poste Italiane** (carte Postepay) occorre interessare il Centro Servizi Bancoposta di Ancona, Accertamenti Patrimoniali – cma – accertamentipatrimoniali2@posteitaliane.it, Tel. 071-4190234/212-----FAX 06/9868470.

Si segnala che Poste Italiane mette a disposizione delle Forze dell'ordine un sistema denominato **PosteAg** per interrogazioni *online* ed in tempo reale su intestatari di conti correnti e carte prepagate di Poste Italiane. Il sistema consente l'accesso a utenti abilitati mediante connessione sicura e l'inserimento di credenziali di autenticazione. Per ottenere il certificato digitale che autorizza l'accesso , il responsabile dell'Ufficio deve inviare un FAX con la richiesta al numero TEL. 0654/922006.

■ Accertamenti su **Paypal** (sistema di pagamento online, utilizzato da eBay) può essere richiesto tramite messaggio alla e-mail forzedellordine@paypal.com, FAX 02/30410366 La sede: PayPal Europe S.a.r.l. & Cie S.C.A. 5° piano 22-24 Boulevard Royal L-2449 Lussemburgo.

Per le carte Paypal (circuito Lottomatica/LIS) è altresì possibile rivolgersi ai seguenti contatti:

- Centralino 06518991;
- ufficiosicurezza@lottomatica.it;
- TEL. 06/51894361.

III) SERVIZIO c.d. DI MONEY TRANSFER:

- **FININT** S.r.l. Milano – Servizio Western Union (ufficio legale):
  - TEL. 02/676261 (centralino);
  - FAX 02/67626601

- Angelo Costa S.r.l. ROMA – Servizio **Western Union**:
  - TEL. 06/87410111 (centralino);
  - FAX 02/67625628;
  - E-mail accertamentiwupsil@legalmail.it

- **American Express** ROMA – Servizio Western Union :
  - FAX 06/7222753 (c.a. D.ssa De Carolis)

  N.B. E' da tenere presente che l'American Express non fornisce più il servizio dalla data del 29 settembre 2009, per cui è da utilizzare unicamente per accertamenti antecedenti tale data.

- **Travelex** ROMA – Servizio Western Union :
  - FAX 06/65872331 (c.a. Sig.ra Ghirardi)

- **Banca di Sassari**, SASSARI – Servizio Western Union:
  - TEL. 079/221511 (centralino);
  - FAX 079/221889 (c.a. dr.ssa Vittoria Sgarella)

- **MoneyGram,** via del Poggio Laurentino 9, 00144 Roma:

- TEL. 06/931831 (centralino);
- FAX 06/83369344

IV) CARTE DI CREDITO:

■ **AMERICAN EXPRESS**:

- TEL. 06/72280605;
- FAX 06/72280188

■ **CARTA SI**:

- TEL. 0234881;
- FAX 0234/884623

■ **VISA**:

- TEL. 0276/29091

V) BANCHE ONLINE

■ **FINECO (Ufficio Relazioni Giudiziarie):**

- TEL. 02/28361 (centralino);
- FAX 02/303482610

■ **IWBANK (UFFICIO Controllo Rischi Operativi ed Antiriciclaggio)**:

- TEL. 02/74874595 (Paola Donato);
- TEL. 02/74874253 (Rosa Martorana);
- FAX 02/74874987;
- TEL. 02/74874111 (centralino)

■ **CHE BANCA (Ufficio Antiriciclaggio – Rapporti con la Magistratura):**

- TEL. 06/54451;

- FAX 02/87287569;
- e-mail indagini.ubis@unicredit.eu

■ **WEBANK (Ufficio Legale):**

- TEL. 02/77001 (centralino);
- FAX 02/43450599

■ **ING DIRECT:**

- TEL. 02/552261;
- FAX 02/55226001

VI) GESTORI TELEFONICI/PROVIDER ITALIANI:

■ **ARUBA:**

- TEL. 0575/0505:
- FAX 0575/862000;
  065/9070010(anagrafica);065/9070011(tabulati);

■ **H3G (portale):**

- TEL. 065/9070000
- FAX 065/9070012 (intercettazioni);
- E-mail arpo.anagrafiche@h3g.legalmail.it;

■ **FASTWEB**:

- TEL. 02/45451;
- FAX 02/45454277

■ **POSTE MOBILE (SIM delle Poste Italiane verso Vodafone):**

- E-mail anagrafiche.postemobile@pec.vodafone.it;
- FAX 800034646

■ **TELECOM / TIM (portale):**

- TEL. 800011577 / TEL. 0228331
- FAX 0269901067; 028356130(telefono); 028356015 (internet)

■ **TISCALI:**

- TEL. 07046011;
- FAX. 070/4609265;
- E-mail rag.tiscali@legalmail.it (scrivere solo tramite pec)

■ **VODAFONE (portale):**

- E-mail ag.web@vodafone.it;
- FAX 800034646; 0683065107 (anagrafica); 0683065108 (tabulati); 0683065109 (intercettazioni)

■ **WIND:**

- TEL. 0683/065100;
- E-mail arp-anagrafica@mail.wind.it

VII) GESTORI AMERICANI/ESTERI:

■ **GOOGLE (YouTube, Gmail, YouPorn, Blogspot):**

- **GOOGLE INC**
1600 Anphitheatre Parkway Mountain View CA 94043 US

TRAMITE

- **GOOGLE ITALIA**
Corso Europa n. 2 Milano
TEL. 0236/618300
FAX 0236/618301

■ **MICROSOFT (HOTMAIL, MSN):**

- **MICROSOFT Corporation**
One Microsoft Way 98052 Redmon WA US

TRAMITE

- MICROSOFT Italia
Centro Direzionale San Felice Palazzo A.
Via Rivoltana n. 13 – 20090 Segrate (MI)
TEL. 0270/3981
FAX 0270/392020

■ **YAHOO!:**

- **YAHOO! Inc.**
701 First Avenue 94089 Sunnyvale CA U.S.

TRAMITE

- **YAHOO! Italia**
Palazzo B – via Spadolini n. 7 20141 Milano
TEL. 0236/653509
FAX 0236/653470

■ **FACEBOOK:**

AUTORITY OPERATION

e-mail subpoena@fb.com

FAX 0236/311375

La società **FACEBOOK** sulla base di un Decreto del Pubblico Ministero italiano tradotto in inglese inviato al suo dipartimento legale, fornisce le seguenti informazioni:

- ☐ Neoprint dell'utente;
- ☐ Photoprint dell'utente;
- ☐ Info di contatto dell'utente;
- ☐ Info su group contact;
- ☐ IP log per un determinato user id o indirizzo ip

■ **SKYPE:**

Communications Sarl, 22/24 Boulevard Royal, L-2449 Luxembourg

- E-mail lerm@skype.net;
- FAX +352 26201582 (infocamere)

CED INTERFORZE?

Cos’è?
Come funziona?

In arrivo aggiornamento su come funziona il ced interforze per il controllo delle persone, con collegamento al sistema shengen (europeo). Su come funziona il riconoscimento facciale + riconoscimenti segni distintivi + approfondimento su rete lan ministero e applicativi usati per intercettazioni.